

Kai-Uwe Schrogl  
*Editor-in-Chief*

SPRINGER  
REFERENCE

Maarten Adriaensen  
Christina Giannopapa  
Peter L. Hays  
Jana Robinson *Section Editors*  
Ntorina Antoni *Managing Editor*

# Handbook of Space Security

Policies, Applications and  
Programs

*Second Edition*

 Springer

---

# Handbook of Space Security

---

Kai-Uwe Schrogl  
Editor-in-Chief

Maarten Adriaensen • Christina  
Giannopapa • Peter L. Hays • Jana Robinson  
Section Editors

Ntorina Antoni  
Managing Editor

# Handbook of Space Security

Policies, Applications and Programs

Second Edition

With 248 Figures and 47 Tables

 Springer

*Editor-in-Chief*

Kai-Uwe Schrogl  
European Space Agency (ESA)  
Paris, France

*Section Editors*

Maarten Adriaensen  
European Space Agency (ESA)  
Paris, France

Christina Giannopapa  
European Space Agency  
(ESA)  
Paris, France

Peter L. Hays  
Space Policy Institute  
George Washington University  
Washington, DC, USA

Jana Robinson  
Space Security Program  
Prague Security Studies  
Institute (PSSI)  
Prague, Czech Republic

*Managing Editor*

Ntorina Antoni  
Eindhoven University of Technology  
Eindhoven, The Netherlands

ISBN 978-3-030-23209-2

ISBN 978-3-030-23210-8 (eBook)

ISBN 978-3-030-23211-5 (print and electronic bundle)

<https://doi.org/10.1007/978-3-030-23210-8>

1st edition: © Springer Science+Business Media New York 2015

2nd edition: © Springer Nature Switzerland AG 2020

All rights are reserved by the Publisher, whether the whole or part of the material is concerned, specifically the rights of translation, reprinting, reuse of illustrations, recitation, broadcasting, reproduction on microfilms or in any other physical way, and transmission or information storage and retrieval, electronic adaptation, computer software, or by similar or dissimilar methodology now known or hereafter developed.

The use of general descriptive names, registered names, trademarks, service marks, etc. in this publication does not imply, even in the absence of a specific statement, that such names are exempt from the relevant protective laws and regulations and therefore free for general use.

The publisher, the authors, and the editors are safe to assume that the advice and information in this book are believed to be true and accurate at the date of publication. Neither the publisher nor the authors or the editors give a warranty, expressed or implied, with respect to the material contained herein or for any errors or omissions that may have been made. The publisher remains neutral with regard to jurisdictional claims in published maps and institutional affiliations.

This Springer imprint is published by the registered company Springer Nature Switzerland AG.  
The registered company address is: Gewerbestrasse 11, 6330 Cham, Switzerland

---

# Introduction

Never before has security in space been more challenged.

Never before has space been more elaborately used for military and security purposes on Earth.

And never before was it more necessary to understand and to receive orientation in the policy area of space security.

This indeed is the purpose of this second edition of the *Handbook of Space Security*, which is addressed to all persons and institutions dealing with space security on a governmental, academic, societal, international, and diplomatic level. From now, the global future will depend on the secure use of outer space for all policy areas with particular stress on climate change and environmental monitoring, telecommunications, navigation, and cyber infrastructures as well as resource management. If space utilization as critical infrastructure is disrupted, our modern societies will break down. Space security is a key factor for survival. This is why space is also contested and space assets are vulnerable.

Consequently, we see a growing “securitization” of outer space. While some decades ago, there were rather clear distinctions between military and civilian uses of space with a smaller area in between called “dual-use.” This zone is ever expanding under the label of “security” diminishing exclusively military and civilian use to small fringes. Just think of environmental security, cyber security, food security, water security, etc., and it becomes clear that we have to speak of a new paradigm also for the use of space. This can also be seen as the most prominent and accelerating development since the publication of the first edition of the Handbook in 2015.

Based on this, the definitional approach we use in this Handbook in space security can be drafted as:

“Space security” is the aggregate of all technical, regulatory and political means that aims to achieve unhindered use of outer space from any interference as well as aims to use space for achieving security on Earth.

This adds to an already existing abundance of definitions for space security. Since it is more than unlikely that a consensus would be reached, our definition stays in the practice of attempting to narrow general applicability and tailor-made approach. For us, it is a frame for the focus and the structure of the Handbook.

The structure of the Handbook comprises four parts. These four parts are edited by accomplished experts in the field. They are Peter L. Hays for Part I International Space Security Setting, Jana Robinson for Part II Space Security Policies and Strategies of States, Maarten Adriaensen for Part III Space Applications and Supporting Services for Security and Defense, and Christina Giannopapa for Part IV Space Security Programs Worldwide and Space Economy Worldwide. They have been assembling exclusive groups of contributors, which do not only reflect a broad geographic distribution (120 authors from 30 countries), but also offer an exciting diversity of practitioners and academics' approaches to the topics. An Editorial Advisory Board of 22 distinguished experts from governments and academia from some 20 countries and every continent (i.e., Africa, Asia, Europe, North America, and South America) assisted the editors in identifying and evaluating contributions to ensure a high-quality, coherent final product.

The Handbook applies political, legal, economic, and technology-oriented analysis to these topics and aims at providing a holistic understanding in each of the sections and for the theme of space security as a whole. It is a work of tertiary literature containing digested knowledge in an easily accessible format. It provides a sophisticated, cutting-edge resource on the space security-related policy portfolio and associated assets to assist fellow members of the global space community, academic audiences, and other interested parties in keeping abreast of the current and future directions of this vital dimension of international space policy. By analyzing the underlying developments in space environment and the linkages to space security from a wide range of disciplines and theoretical perspectives, this Handbook establishes itself as a leading work for reference purposes, as well as a basis for further discussion.

Furthermore, it is enriched by the account of numerous space operational applications that routinely deliver indispensable fast and reliable services for security and defense needs from and for space. The transformation of the space domain through new technological advances and types of innovation such as mega-constellations, machine learning, and artificial intelligence has resulted in major challenges. Finally, it examines how addressing these needs has led to space programs and the development of specific security space assets. In short, it examines the reciprocal relations among space policy objectives on one hand and operational capabilities on the other, allowing readers to understand the theoretical and practical interactions and limitations between them. It also features numerous recommendations concerning how to best improve the space security environment, given the often-competing objectives of the world's major space-faring nations.

The Handbook is available in both printed and electronic forms. Its success is documented by more than 100,000 chapter downloads for its first edition. The Handbook is intended to assist and promote both academic research and professional activities in this rapidly evolving field encompassing security from and for space. It aspires to remain a go-to reference manual for space policy practitioners and decision makers, scholars, students, researchers, and experts as well as the media. The Springer Publishing House has been an exemplary partner in this major undertaking. We would like to gratefully acknowledge the cooperation of Maury Solomon

---

and Hannah Kaufmann (New York), Lydia Muller (Heidelberg), Juby George, and Sonal Nagpal (New Delhi). Ntorina Antoni, the Managing Editor of the Handbook, acted as the invaluable main liaison between our editorial team, contributors, and publisher throughout the project. It is the hope of all of us who joined together to prepare this second edition of the *Handbook of Space Security* that it will inspire those seeking to be active in shaping space security, on which we all depend.

September 2020

Kai-Uwe Schrogl  
Editor-in-Chief

---

## Advisory Board

- Setsuko Aoki** Professor of Law, Keio University Law School, Tokyo, Japan  
Chair, United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) Legal Subcommittee, Vienna, Austria  
Vice President, International Institute of Space Law (IISL), Paris, France
- Natália Archinard** Deputy Head of the Education, Science, Transport and Space Section, Directorate of Political Affairs, Federal Department of Foreign Affairs, Berne, Switzerland  
Chair, UNCOPUOS Scientific and Technical Subcommittee, Vienna, Austria
- Frank Asbeck** Senior Fellow at the Prague Security Studies Institute (PSSI), Prague, Czech Republic  
Former Principle Adviser for Space and Security Policy, European External Action Service (EEAS), Brussels, Belgium  
Former Director of the European Union Satellite Centre (EU SatCen), Torrejon, Spain
- Tare Brisibe** Senior Legal and Regulatory Counsel, Asia-Pacific, SES, Singapore  
Former Chair, UNCOPUOS Legal Subcommittee, Vienna, Austria  
Former Deputy Director (Legal) National Space Research and Development Agency of Nigeria, Lagos, Nigeria
- Gerard Brachet** Space Policy Consultant, Paris, France  
Former Chair, UNCOPUOS, Vienna, Austria  
Former Director General, French Space Agency – CNES, Paris, France



<b>Alice Bunn</b>	International Director, UK Space Agency, Swindon, United Kingdom Co-Chair, Global Future Council on Space Technology, World Economic Forum, Cologny, Switzerland
<b>Michael Davis</b>	Former Chair, Space Industry Association of Australia (SIAA), Golden Grove Village, Australia
<b>Simonetta Di Pippo</b>	Director, United Nations Office for Outer Space Affairs (UNOOSA), Vienna, Austria
<b>Monserrat Filho</b>	Head, International Affairs Office of the Ministry of Science and Technology, Brasilia, Brazil
<b>Driss El Hadani</b>	Director, Royal Centre for Remote Sensing (CRTS), Rabat, Morocco
<b>Armel Kerrest</b>	Emeritus Professor of Public Law at the Universities of Western Brittany, Brest and Paris XI, France Vice Chairman, European Centre for Space Law of the European Space Agency (ECSL/ESA), Paris, France
<b>Pascal Legai</b>	Senior Adviser – Earth Observation to the European Space Agency (ESA), Frascati, Italy Former Director, European Union Satellite Centre (EU SatCen), Torrejon, Spain
<b>Sergio Marchisio</b>	Professor of International Law and Space Law, Sapienza University of Rome, Italy Chair, European Centre for Space Law (ECSL/ESA), Paris, France
<b>Marian-Jean Marinescu</b>	Member, European Parliament, Coordinator for Transport Policies, EPP Group Romania, Brussels, Belgium Chair, Sky and Space Intergroup in the European Parliament, Brussels, Belgium
<b>Martha Mejía-Kaiser</b>	Independent Researcher, Mexico/Germany Member of the Board of Directors, International Institute of Space Law (IISL), Paris, France
<b>K.R. Sridhara Murthi</b>	Professor of Aerospace Engineering and Management, Jain University, Bangalore, India Vice President, International Institute of Space Law (IISL), Paris, France
<b>Rosa Ma. Ramírez de Arellano y Haro</b>	General Director of International Affairs and Space Security at the Mexican Space Agency, Mexico City, Mexico Former Chair, UNCOPUOS and UNISPACE+50, Vienna, Austria
<b>Michael Simpson</b>	Former Executive Director, Secure World Foundation, Colorado Springs, USA Former President, International Space University (ISU), Strasbourg, France

- 
- Li Shouping** General-Director, Space Law Center of China National Space Administration (CNSA), Haidian District, Beijing, China  
Dean, Law School of Beijing Institute of Technology, Beijing, China
- Paul Weissenberg** Senior Advisor to the Executive Director of the European GNSS Agency (GSA), Prague, Czech Republic  
Senior Advisor, The European External Action Service (EEAS), Brussels, Belgium  
Senior Advisor, The European Commission DG GROW, Brussels, Belgium  
Former Deputy Director General, European Commission for the Galileo and Copernicus space programs and Security and Defence Industries, Brussels, Belgium
- Klaus-Peter Willsch** Member of the German Parliament (Deutscher Bundestag), Berlin, Germany  
Chair of the aerospace group in the German Parliament, Berlin, Germany  
Former Chair, European Interparliamentary Space Committee (EISC)
- Viktor Veshchnuvov** Executive Director, Intersputnik International Organization of Space Communications, Moscow, Russian Federation

---

# Contents

## Volume 1

<b>Part I International Space Security Setting</b> .....	<b>1</b>
<b>1 International Space Security Setting: An Introduction</b> .....	<b>3</b>
Peter L. Hays	
<b>2 Definition and Status of Space Security</b> .....	<b>9</b>
Ntorina Antoni	
<b>3 Challenges to International Space Governance</b> .....	<b>35</b>
Ahmad Khan and Sufian Ullah	
<b>4 Spacepower Theory and Organizational Structures</b> .....	<b>49</b>
Peter L. Hays	
<b>5 The Laws of War in Outer Space</b> .....	<b>73</b>
Steven Freeland and Elise Gruttner	
<b>6 Arms Control and Space Security</b> .....	<b>95</b>
Stacey Henderson	
<b>7 Role of Space in Deterrence</b> .....	<b>111</b>
John J. Klein and Nickolas J. Boensch	
<b>8 Resilience of Space Systems: Principles and Practice</b> .....	<b>127</b>
Regina Peldszus	
<b>9 Space Security Cooperation: Changing Dynamics</b> .....	<b>145</b>
Jessica L. West	
<b>10 Strategic Competition for Space Partnerships and Markets</b> .....	<b>163</b>
Jana Robinson, Tereza B. Kupková, and Patrik Martínek	
<b>11 Space Export Control Law and Regulations</b> .....	<b>185</b>
Ulrike M. Bohlmann and Gina Petrovici	
<b>12 Space Systems and Space Sovereignty as a Security Issue</b> .....	<b>211</b>
Annamaria Nassisi and Isabella Patatti	

<b>13</b>	<b>Critical Space Infrastructures</b> .....	227
	Alexandru Georgescu	
<b>14</b>	<b>Space and Cyber Threats</b> .....	245
	Stefano Zatti	
<b>15</b>	<b>Space Safety</b> .....	265
	Joe Pelton, Tommaso Sgobba, and Maite Trujillo	
<b>16</b>	<b>Evolution of Space Traffic and Space Traffic Management</b> .....	299
	William Ailor	
<b>17</b>	<b>Space Sustainability</b> .....	319
	Peter Martinez	
<b>18</b>	<b>Security Issues with Respect to Celestial Bodies</b> .....	341
	George D. Kyriakopoulos	
<b>Part II</b>	<b>Space Security Policies and Strategies of States</b> .....	<b>357</b>
<b>19</b>	<b>Space Security Policies and Strategies of States: An Introduction</b> ...	359
	Jana Robinson	
<b>20</b>	<b>War, Policy, and Spacepower: US Space Security Priorities</b> .....	367
	Everett C. Dolman	
<b>21</b>	<b>Russia's Space Security Policy</b> .....	385
	Nicole J. Jackson	
<b>22</b>	<b>Development of a Space Security Culture: Case of Western European Union</b> .....	401
	Alexandros Kolovos	
<b>23</b>	<b>Strategic Overview of European Space and Security Governance</b> .....	421
	Ntorina Antoni, Maarten Adriaensen, and Christina Giannopapa	
<b>24</b>	<b>European Space Security Policy: A Cooperation Challenge for Europe</b> .....	449
	Jean-Jacques Tortora and Sebastien Moranta	
<b>25</b>	<b>Space and Security Policy in Selected European Countries</b> .....	467
	Ntorina Antoni, Maarten Adriaensen, and Christina Giannopapa	
<b>26</b>	<b>Poland and Space Security</b> .....	485
	Małgorzata Polkowska	
<b>27</b>	<b>Space Security in the Asia-Pacific</b> .....	499
	Rajeswari Pillai Rajagopalan	
<b>28</b>	<b>Chinese Space and Security Policy: An Overview</b> .....	515
	Zhuoyan Lu	

<b>29 Chinese Concepts of Space Security: Under the New Circumstances</b> .....	527
Dean Cheng	
<b>30 Historical Evolution of Japanese Space Security Policy</b> .....	555
Kazuto Suzuki	
<b>31 India in Space: A Strategic Overview</b> .....	571
Ajey Lele	
<b>32 Israel’s Approach Towards Space Security and Sustainability</b> ...	589
Deaganit Paikowsky, Tal Azoulay, and Isaac Ben Israel	
<b>33 Policies and Programs of Iran’s Space Activities</b> .....	601
Hamid Kazemi and Mahshid TalebianKiakalayeh	
<b>34 UAE Approach to Space and Security</b> .....	621
Naser Al Rashedi, Fatima Al Shamsi, and Hamda Al Hosani	
<b>35 Space Security in Brazil</b> .....	653
Olavo de O. Bittencourt Neto and Daniel Freire e Almeida	
<b>36 Space and Security Activities in Azerbaijan</b> .....	667
Tarlan Mammadzada	

**Volume 2**

<b>Part III Space Applications and Supporting Services for Security and Defense</b> .....	<b>699</b>
<b>37 Introduction to Space Applications and Supporting Services for Security and Defense</b> .....	701
Maarten Adriaensen	
<b>38 Earth Observation for Security and Defense</b> .....	705
Ferdinando Dolce, Davide Di Domizio, Denis Bruckert, Alvaro Rodríguez, and Andrea Patrono	
<b>39 Satellite EO for Disasters, Risk, and Security: An Evolving Landscape</b> .....	733
Helene de Boissezon and Andrew Eddy	
<b>40 Space-Enabled Systems for Food Security in Africa</b> .....	759
Olufunke Adebola and Simon Adebola	
<b>41 Satellite Communication for Security and Defense</b> .....	779
Holger Lueschow and Roberto Pelaez	
<b>42 Position, Navigation, and Timing for Security</b> .....	797
Jean-Christophe Martin	

<b>43</b>	<b>PNT for Defense</b> .....	821
	Marco Detratti and Ferdinando Dolce	
<b>44</b>	<b>Space Traffic Management Through Environment Capacity</b> .....	845
	Stijn Lemmens and Francesca Letizia	
<b>45</b>	<b>Various Threats of Space Systems</b> .....	865
	Xavier Pasco	
<b>46</b>	<b>European Space Surveillance and Tracking Support Framework</b> .....	883
	Regina Peldszus and Pascal Faucher	
<b>47</b>	<b>China's Capabilities and Priorities in Space-Based Safety and Security Applications</b> .....	905
	Lin Shen, Hongbo Li, Shengjun Zhang, and Xin Wang	
<b>48</b>	<b>Cybersecurity Space Operation Center: Countering Cyber Threats in the Space Domain</b> .....	921
	Salvador Llopis Sanchez, Robert Mazzolin, Ioannis Kechaoglou, Douglas Wiemer, Wim Mees, and Jean Muylaert	
<b>49</b>	<b>AI and Space Safety: Collision Risk Assessment</b> .....	941
	Luis Sanchez, Massimiliano Vasile, and Edmondo Minisci	
<b>50</b>	<b>Space Object Behavior Quantification and Assessment for Space Security</b> .....	961
	Moriba Jah	
<b>51</b>	<b>Space Security and Frequency Management</b> .....	985
	Yvon Henri and Attila Matas	
<b>52</b>	<b>Space Weather: The Impact on Security and Defense</b> .....	1005
	Jan Janssens, David Berghmans, Petra Vanlommel, and Jesse Andries	
<b>53</b>	<b>Space Security in the Context of Cosmic Hazards and Planetary Defense</b> .....	1025
	Joe Pelton	
<b>54</b>	<b>Active Debris Removal for Mega-constellation Reliability</b> .....	1043
	Nikita Veliev, Anton Ivanov, and Shamil Biktimirov	
<b>55</b>	<b>Space Security and Sustainable Space Operations: A Commercial Satellite Operator Perspective</b> .....	1063
	Jean François Bureau	
<b>56</b>	<b>Space Debris Mitigation Systems: Policy Perspectives</b> .....	1079
	Annamaria Nassisi, Gaia Guiso, Maria Messina, and Cristina Valente	

<b>57 Security Exceptions to the Free Dissemination of Remote Sensing Data: Interactions Between the International, National, and Regional Levels</b> .....	1091
Philip De Man	
 <b>Part IV Space Security Programs Worldwide and Space Economy Worldwide</b> .....	<b>1123</b>
<b>58 Space Security Programs and Space Economy: An Introduction</b> ...	1125
Christina Giannopapa	
<b>59 Satellite Programs in the USA</b> .....	1133
Pat Norris	
<b>60 Russian Space Launch Program</b> .....	1171
Elina Morozova	
<b>61 Institutional Space Security Programs in Europe</b> .....	1191
Ntorina Antoni, Maarten Adriaensen, and Christina Giannopapa	
<b>62 Space and Security Programs in the Largest European Countries</b> .....	1225
Ntorina Antoni, Christina Giannopapa, and Maarten Adriaensen	
<b>63 Space and Security Programs in Medium-Sized European Countries</b> .....	1265
Ntorina Antoni, Christina Giannopapa, and Maarten Adriaensen	
<b>64 Space and Security Programs in Smaller European Countries</b> ...	1289
Ntorina Antoni, Christina Giannopapa, and Maarten Adriaensen	
<b>65 Future of French Space Security Programs</b> .....	1329
Jean-Daniel Testé	
<b>66 Italy in Space: Strategic Overview and Security Aspects</b> .....	1343
Francesco Pagnotta and Marco Reali	
<b>67 British Spacepower: Context, Policies, and Capabilities</b> .....	1365
Bleddyn Bowen	
<b>68 Chinese Satellite Program</b> .....	1381
Xiaoxi Guo	
<b>69 Chinese Space Launch Program</b> .....	1401
Lehao Long, Lin Shen, Dan Li, Hongbo Li, Dong Zeng, and Shengjun Zhang	
<b>70 Indian Space Program: Evolution, Dimensions, and Initiatives</b> ...	1421
Hanamantray Baluragi and Byrana Nagappa Suresh	
<b>71 Australia’s Space Security Program</b> .....	1441
Michael Davis and Chris Schacht	

---

<b>72</b>	<b>Pakistan's Space Activities</b> .....	1455
	Ahmad Khan, Tanzeela Khalil, and Irteza Imam	
<b>73</b>	<b>Space Sector Economy and Space Programs World Wide</b> .....	1471
	Per Høyland, Estelle Godard, Marta De Oliveira, and Christina Giannopapa	
<b>74</b>	<b>The New Space Economy: Consequences for Space Security in Europe</b> .....	1499
	Jean-Pierre Darnis	
<b>75</b>	<b>Political Economy of Outer Space Security</b> .....	1511
	Vasilis Zervos	
<b>76</b>	<b>Views on Space Security in the United Nations</b> .....	1535
	Massimo Pellegrino	
<b>77</b>	<b>The Role of COSPAR for Space Security and Planetary Protection</b> .....	1559
	Leslie I. Tennen	
<b>Index</b>	.....	1581



---

## About the Editor-in-Chief



**Prof. Dr. Kai-Uwe Schrogl** is currently seconded from the European Space Agency (ESA) to the German Federal Ministry for Economic Affairs and Energy in Berlin to support the preparation of the German Presidency of the Council of the European Union in the second half of 2020. Until 2019, Dr. Schrogl was the Chief Strategy Officer of ESA (Headquartered in Paris, France). From 2007 to 2011 he was the Director of the European Space Policy Institute (ESPI) in Vienna, Austria, the leading European think tank for space policy. Prior to this, he was the Head of the Corporate Development and External Relations Department in the German Aerospace Center (DLR) in Cologne, Germany. Previously, he also worked with the German Ministry for Post and Telecommunications and the German Space Agency (DARA) in Bonn, Germany. Dr. Schrogl has been a delegate to numerous international forums and has served from 2014 to 2016 as Chairman of the Legal Subcommittee of the United Nations Committee on the Peaceful Uses of Outer Space, the highest body for space law making, comprising 73 Member States. He also was chairman of various European and global committees (ESA International Relations Committee and two plenary working groups of the UNCOPUOS Legal Subcommittee, the one on the launching State and the other on the registration practice, both leading to UN General Assembly Resolutions).

He presented, respectively testified, at hearings of the European Parliament and the U.S. House of Representatives. Dr. Schrogl is President of the International Institute of Space Law, the professional association of space law experts from 48 countries, Member of the International Academy of Astronautics (recently chairing its Commission on policy, economics, and

regulations) and the Russian Academy of Cosmonautics, as well as Corresponding Member of the French Air and Space Academy. He holds a doctorate degree in political science and lectures international relations as an Honorary Professor at Tübingen University, Germany. Dr. Schrogl has written or co-edited 17 books and more than 140 articles, reports, and papers in the fields of space policy and law as well as telecommunications policy. He launched and edited until 2011 the *Yearbook on Space Policy* and the book series *Studies in Space Policy*, both published by ESPI at Springer-WienNewYork. He sits on editorial boards of various international journals in the field of space policy and law (*Space Policy*, *Zeitschrift für Luft- und Weltraumrecht*, *Studies in Space Law/Nijhoff*; previously also *Acta Astronautica*).

---

## About the Section Editors



**Maarten Adriaensen** currently works for the Procurement Department of the European Space Agency (ESA) in Paris, France. He was previously seconded by the ESA to the European Defence Agency (EDA) in Brussels, Belgium, assigned as Policy Officer Space. In that function, he provided strategic analysis and synthesis in support of EDA Directorates, internal coordination of EDA space activities, and support to cooperation on space activities externally. Prior to that, Maarten Adriaensen worked in the Procurement Department and Policy Department of ESA in Paris; the University of Leuven, Belgium; and the European Space Policy Institute (ESPI) in Vienna, Austria. He holds an M.Sc. in Space Studies (cum laude), M.A. in European Studies: Transnational and Global Perspectives (magna cum laude), M.A. in Modern History (cum laude), LLB, and an Academic Teacher Degree from the University of Leuven. He attended the 2012 International Space University (ISU) Space Studies Program (SSP) in Florida, hosted by the Florida Institute of Technology and NASA Kennedy Space Center. The content of Maarten's contributions to the Handbook reflect his personal opinions and do not necessarily reflect the opinion of the European Space Agency.



**Dr. Christina Giannopapa** works at the European Space Agency (ESA) since 2007. Currently, she is seconded from ESA to the Greek Ministry of Digital Policy, Telecommunications and Media as Special Advisor on high-tech and space applications related issues. Until February 2019, Dr. Giannopapa has been ESA's Head of Political Affairs Office in the Strategy Department of the Director General's Services in Paris, being responsible for providing advice and support on political matters to the Director General. From 2012 to 2015, she has been working on Member States Relations Department of ESA. From 2010 to 2012, Dr. Giannopapa has been seconded from the Agency as Resident Fellow at the European Space Policy Institute (ESPI) in Vienna, where she has been supporting the European Interparliamentary Space Conference (EISC) and lead studies on innovation, Galileo, Copernicus, and Africa. In the policy areas she also worked briefly in DG Research, European Commission. From 2007 to 2010, Dr. Giannopapa has been working in the Mechanical Engineering Department of the Technical and Quality Management Directorate of ESA in the Netherlands. Prior to joining ESA, she has worked as a consultant to high-tech industries in research and technology development. Dr. Giannopapa held positions in academia in Eindhoven University of Technology, the Netherlands, and in the University of London, UK. She has received 14 academic scholarships and awards and has more than 60 publications in peer-reviewed journals and conferences. Dr. Giannopapa holds a Ph.D. in Engineering and Applied Mathematics, an M.Eng. in Manufacturing Systems Engineering and Mechatronics, and an M.B.A. in International Management from the University of London, UK. Additionally, she is Assistant Professor in the Department of Industrial Engineering and Innovation Sciences at Eindhoven University of Technology. Dr. Giannopapa is the Chairperson of the Committee for Liaison with International Organisations and Developing Nations (CLIODN) and the Secretary of the Space Security Committee of the International Astronautical Federation (IAF). She is also the Director for Professional Development of Women in Aerospace-Europe (WIA-E).



**Peter L. Hays** is an Adjunct Professor at George Washington University's (GWU) Space Policy Institute and a Senior Policy Advisor with Falcon Research. He has been directly involved in helping to develop and implement major national security space policy initiatives since 2004 and serves as a senior advisor on governance, cadre, and strategic messaging issues. Peter served as a Staff Augmentee at the Office of Science and Technology Policy in 1988 and at the National Space Council in 1990. He served as an Air Force Officer from 1979 to 2004, flew C-141 cargo planes, and previously taught at the Air Force Academy, Air Force School of Advanced Airpower Studies, and National Defense University; he now teaches Air- and Spacepower Seminars at the Marine Corps School of Advanced Warfighting and the Space and National Security and the Science, Technology, and National Security Policy graduate seminars at GWU. Peter holds a Ph.D. from the Fletcher School and was an Honor Graduate of the Air Force Academy. Major publications include: *Handbook of Space Security, Space and Security*, and *Toward a Theory of Spacepower*.



**Dr. Jana Robinson** is Space Security Program Director at the Prague Security Studies Institute (PSSI). She previously served as a Space Policy Officer at the European External Action Service (EEAS) in Brussels as well as a Space Security Advisor to the Czech Foreign Ministry. From 2009 to 2013, Dr. Robinson worked at the European Space Policy Institute (ESPI), seconded from the European Space Agency (ESA), leading the Institute's Space Security Research Programme. Dr. Robinson is an elected member of the International Institute of Space Law (IISL) and the International Academy of Astronautics (IAA). She is also a member of the Advisory Board of the George C. Marshall Missile Defense Project of the Center for Strategic and International Studies (CSIS) in Washington, D.C. Dr. Robinson holds a Ph.D. in Space Security from Charles University in Prague and received two M.A. degrees from George Washington University's Elliott School of International Affairs and Palacky University in Olomouc, respectively.

---

## About the Managing Editor



**Ntorina Antoni** is currently a Ph.D. candidate of strategic management in space security at Eindhoven University of Technology. Her research focuses on strategic decision-making under uncertainty and legitimacy in the context of high reliability organizations. She is also an Attorney-at-Law and member of the Athens Bar Association in Greece. Ntorina previously worked at the Strategy Department of the European Space Agency (ESA). In her role as Strategy and Policy Analyst, she got involved in the research and analysis of regulations, policies, and strategies of the ESA member states. Prior to that, Ntorina served as the Legal Counsel for Swiss Space Systems, a company which planned to provide orbital launches of small satellites and manned sub-orbital spaceflights. She was in charge of the legal and regulatory aspects of aviation and aerospace projects including aircraft purchase, certification of parabolic flights and suborbital flights, as well as regulation of small satellites. Ntorina is a Board Member of the Brainport TechLaw in Eindhoven and an elected member of the International Institute of Space Law (IISL). She holds a Law degree from the University of Athens in Greece, a Master's degree (LL.M) in International and European Law from Tilburg University in the Netherlands, and an Advanced Master's degree (LL.M) in Air and Space Law from Leiden University in the Netherlands.

---

## Contributors

**Olufunke Adebola** Sam Nunn School of International Affairs, Georgia Institute of Technology, Atlanta, GA, USA

**Simon Adebola** Capacity Direct LLC, Atlanta, USA

**Maarten Adriaensen** European Space Agency (ESA), Paris, France

**William Ailor** Center for Orbital and Reentry Debris Studies, The Aerospace Corporation, El Segundo, CA, USA

**Hamda Al Hosani** Space Policies and Legislations Department, UAE Space Agency, Masdar City, Abu Dhabi, United Arab Emirates

**Naser Al Rashedi** Space Policies and Legislations Department, UAE Space Agency, Masdar City, Abu Dhabi, United Arab Emirates

**Fatima Al Shamsi** Space Policies and Legislations Department, UAE Space Agency, Masdar City, Abu Dhabi, United Arab Emirates

**Jesse Andries** Solar Terrestrial Center of Excellence (STCE) – Solar Influences Data Analysis Center (SIDC), Royal Observatory of Belgium, Brussels, Belgium

**Ntorina Antoni** Eindhoven University of Technology, Eindhoven, The Netherlands

**Tal Azoulay** Yuval Neeman Workshop for Science, Technology and Security, Tel Aviv University, Tel Aviv, Israel

**Hanamantray Baluragi** Indian Space Research Organization (ISRO), Bangalore, India

**David Berghmans** Solar Terrestrial Center of Excellence (STCE) – Solar Influences Data Analysis Center (SIDC), Royal Observatory of Belgium, Brussels, Belgium

**Shamil Biktimirov** Skolkovo Institute of Science and Technology, Moscow, Russia

**Olavo de O. Bittencourt Neto** Catholic University of Santos, Santos, Brazil

**Nickolas J. Boensch** Bryce Space and Technology, Alexandria, VA, USA

- Ulrike M. Bohlmann** European Space Agency (ESA), Paris, France
- Bleddyn Bowen** University of Leicester, Leicester, UK
- Denis Bruckert** EU Satellite Centre (EUSC), Madrid, Spain
- Jean François Bureau** Institutional and International Affairs, Eutelsat Group VP, Paris, France
- Dean Cheng** The Heritage Foundation, Washington, DC, USA
- Jean-Pierre Darnis** Université Côte d’Azur, Istituto Affari Internazionali, (IAI), Nice, France
- Michael Davis** Space Industry Association of Australia, Adelaide, Australia
- Helene de Boissezon** French Space Agency (CNES), Toulouse, France  
Committee on Earth Observation Satellites (CEOS), Haiti Recovery Observatory, Port au Prince, Haiti
- Philip De Man** University of Sharjah, Sharjah, UAE  
University of Leuven, Leuven, Belgium
- Marta De Oliviera** International Space University (ISU), Illkirch-Graffenstaden, France
- Marco Detratti** European Defence Agency (EDA), Brussels, Belgium
- Davide Di Domizio** European Defence Agency (EDA), Brussels, Belgium
- Ferdinando Dolce** European Defence Agency (EDA), Brussels, Belgium
- Everett C. Dolman** Air Command and Staff College, Air University, Montgomery, AL, USA
- Andrew Eddy** Athena Global, Simiane-la-Rotonde, France
- Pascal Faucher** Defence and Security Office, French Space Agency (CNES), Paris, France
- Steven Freeland** University of Western Sydney, Sydney, NSW, Australia
- Daniel Freire e Almeida** Catholic University of Santos, Santos, Brazil
- Alexandru Georgescu** National Institute for Research and Development in Informatics (ICI), Bucharest, Romania
- Christina Giannopapa** European Space Agency (ESA), Paris, France
- Estelle Godard** Institut d’études politiques de Paris, Paris, France
- Elise Gruttner** United Nations Assistance to the Khmer Rouge Trials, New York, NY, USA
- Gaia Guiso** Women in Aerospace-Europe (WIA-E), Milan, Italy



**Xiaoxi Guo** China Academy of Space Technology (CAST), Beijing, People's Republic of China

**Peter L. Hays** Space Policy Institute, George Washington University, Washington, DC, USA

**Stacey Henderson** Adelaide Law School, The University of Adelaide, Adelaide, SA, Australia

**Yvon Henri** OneWeb, London, UK

**Per Høyland** Department of Political Science, University of Oslo, Oslo, Norway

**Irteza Imam** Department of Defence and Strategic Studies, Quaid-i-Azam University, Islamabad, Pakistan

**Isaac Ben Israel** Yuval Neeman Workshop for Science, Technology and Security, Tel Aviv University, Tel Aviv, Israel

**Anton Ivanov** Skolkovo Institute of Science and Technology, Moscow, Russia

**Nicole J. Jackson** School for International Studies, Simon Fraser University, Vancouver, BC, Canada

**Moriba Jah** Department of Aerospace Engineering and Engineering Mechanics, The University of Texas at Austin, Austin, TX, USA

**Jan Janssens** Solar Terrestrial Center of Excellence (STCE) – Solar Influences Data Analysis Center (SIDC), Royal Observatory of Belgium, Brussels, Belgium

**Hamid Kazemi** Aerospace Research Institute, Department of Air and Space Law, Tehran, Iran

**Ioannis Kechaoglou** RHEA Group, Wavre, Belgium

**Tanzeela Khalil** South Asia Center, Atlantic Council, Washington, DC, USA

**Ahmad Khan** Department of Strategic Studies, National Defence University, Islamabad, Pakistan

**John J. Klein** George Washington University's Space Policy Institute, Washington, DC, USA

**Alexandros Kolovos** Automatic Control, AirSpace Technology, Defence Systems and Operations Section, Hellenic Air Force Academy, Athens, Greece

**Tereza B. Kupková** Prague Security Studies Institute (PSSI), Prague, Czech Republic

**George D. Kyriakopoulos** School of Law, National and Kapodistrian University of Athens, Athens, Greece

**Ajey Lele** Institute for Defence Studies and Analyses, New Delhi, India

**Stijn Lemmens** Space Debris Office, European Space Agency (ESA) – European Space Operations Centre (ESOC), Darmstadt, Germany

**Francesca Letizia** Space Debris Office, IMS Space Consultancy at Space Debris Office, European Space Agency (ESA) – European Space Operations Centre (ESOC), Darmstadt, Germany

**Hongbo Li** China Academy of Launch Vehicle Technology (CALT), Beijing, China

**Dan Li** China Academy of Launch Vehicle Technology (CALT), Beijing, China

**Salvador Llopis Sanchez** European Defence Agency (EDA), Brussels, Belgium

**Lehao Long** Chinese Academy of Engineering, Beijing, China

**Zhuoyan Lu** International Space University (ISU), Strasbourg, France

**Holger Lueschow** European Defence Agency (EDA), Brussels, Belgium

**Tarlan Mammadzada** “Azercosmos” OJSCo, Baku, Azerbaijan

**Patrik Martínek** The Prague Security Studies Institute (PSSI), Prague, Czech Republic

**Jean-Christophe Martin** CEO Marency SAS, Paris, France  
CEO Marency SAS, Brussels, Belgium

**Peter Martinez** Secure World Foundation (SWF), Broomfield, CO, USA

**Attila Matas** Orbit/Spectrum Consulting, Grand-Saconnex, Switzerland

**Robert Mazzolin** RHEA Group, Wavre, Belgium

**Wim Mees** Royal Military Academy, Brussels, Belgium

**Maria Messina** Education Unit, Italian Space Agency (ASI), Rome, Italy

**Edmondo Minisci** University of Strathclyde, Glasgow, UK

**Sebastien Moranta** European Space Policy Institute (ESPI), Vienna, Austria

**Elina Morozova** International Legal Service, Intersputnik International Organization of Space Communications, Moscow, Russian Federation  
International Institute of Space Law, Paris, France

**Jean Muylaert** RHEA Group, Wavre, Belgium

**Annamaria Nassisi** Strategic Marketing, Thales Alenia Space, Rome, Italy

**Pat Norris** VAPN Ltd, West Byfleet, UK

**Francesco Pagnotta** Presidency of the Council of Ministers – Office of the Military Advisor, Rome, Italy

**Deganit Paikowsky** Yuval Neeman Workshop for Science, Technology and Security, Tel Aviv University, Tel Aviv, Israel

**Xavier Pasco** Fondation pour la Recherche Stratégique (FRS), Paris, France

**Isabella Patatti** Strategic Marketing, Thales Alenia Space, Rome, Italy

**Andrea Patrono** EU Satellite Centre (EUSC), Madrid, Spain

**Roberto Pelaez** European Defence Agency (EDA), Brussels, Belgium

**Regina Peldszus** Department of Space Situational Awareness, German Aerospace Center (DLR) Space Administration, Bonn, Germany

**Massimo Pellegrino** Vienna, Austria

**Joe Pelton** International Association for the Advancement of Space Safety (IAASS), Arlington, VA, USA

**Gina Petrovici** German Aerospace Center (DLR), Bonn, Germany

**Malgorzata Polkowska** University of War Studies, Warsaw, Poland

**Rajeswari Pillai Rajagopalan** Nuclear and Space Policy Initiative, Observer Research Foundation, New Delhi, India

**Marco Reali** Presidency of the Council of Ministers – Office of the Military Advisor, Rome, Italy

**Jana Robinson** Space Security Program, Prague Security Studies Institute (PSSI), Prague, Czech Republic

**Alvaro Rodríguez** EU Satellite Centre (EUSC), Madrid, Spain

**Luis Sanchez** University of Strathclyde, Glasgow, UK

**Chris Schacht** Adelaide, Australia

**Tommaso Sgobba** International Association for the Advancement of Space Safety (IAASS), Noordwijk, The Netherlands

**Lin Shen** China Academy of Launch Vehicle Technology (CALT), Beijing, China

**Byrana Nagappa Suresh** Indian Space Research Organization (ISRO), Bangalore, India

**Kazuto Suzuki** Hokkaido University, Hokkaido, Japan

**Mahshid TalebianKiakalayah** Graduate of Islamic Azad University, Tehran North Branch, Tehran, Iran

**Leslie I. Tennen** Law Offices of Sterns and Tennen, Glendale, AZ, USA

**Jean-Daniel Testé** OTA (l'Observation de la Terre Appliquée), Peujard, France

**Jean-Jacques Tortora** European Space Policy Institute (ESPI), Vienna, Austria

---

**Maite Trujillo** European Space Agency (ESA) – European Space Research and Technology Centre (ESTEC), Noordwijk, The Netherlands

**Sufian Ullah** Department of Defence and Strategic Studies, Quaid-i-Azam University, Islamabad, Pakistan

**Cristina Valente** Marketing and Sales, Telespazio, Rome, Italy

**Petra Vanlommel** Solar Terrestrial Center of Excellence (STCE) – Solar Influences Data Analysis Center (SIDC), Royal Observatory of Belgium, Brussels, Belgium

**Massimiliano Vasile** University of Strathclyde, Glasgow, UK

**Nikita Veliev** Skolkovo Institute of Science and Technology, Moscow, Russia

**Xin Wang** China Academy of Launch Vehicle Technology (CALT), Beijing, China

**Jessica L. West** Project Ploughshares, Waterloo, ON, Canada

**Douglas Wiemer** RHEA Group, Wavre, Belgium

**Stefano Zatti** European Space Agency (ESA) – Security Office, Frascati, Italy

**Dong Zeng** China Academy of Launch Vehicle Technology (CALT), Beijing, China

**Vasilis Zervos** University of Strasbourg and International Space University (ISU), Strasbourg, France

**Shengjun Zhang** China Academy of Launch Vehicle Technology (CALT), Beijing, China

---

**Part I**

**International Space Security Setting**



# International Space Security Setting: An Introduction

1

Peter L. Hays

## Contents

Foundational Themes .....	3
International Space Security Focus Areas .....	5
Conclusions .....	7

## Abstract

This chapter provides an introduction to Part 1 of the second edition of the *Handbook of Space Security* by overviewing major issues and themes that frame discourse about space security. This part contains 17 chapters that include foundational discussions about definitional, governance, theoretical, legal, deterrence, and resilience themes for space security as well as more focused discussions about cooperation, strategic competition, export controls, critical infrastructure, cyber threats, safety, traffic management, and the sustainability of space resources. Together, these themes and issues provide a comprehensive setting for refining and advancing our dialogue about international space security.

## Foundational Themes

Defining and scoping space security has been and still probably is the single most important issue for any dialogue about this topic. While some decades ago most distinctions between military and civilian uses of space were rather clear, there was always an area in between called “dual-use.” The latter has been ever expanding under the label of “security” and it has thereby been diminishing exclusively military and civilian purposes to just small remnants. One can think of the challenges that arise in the fields of environmental security, cybersecurity, food security, water

P. L. Hays (✉)

Space Policy Institute, George Washington University, Washington, DC, USA

e-mail: [hayspl@gwu.edu](mailto:hayspl@gwu.edu)

security, and other areas. Tackling the security issues in these domains requires analysts to take into consideration all dual-use elements that serve both civilian and military uses. It then becomes clear that we must speak of a new paradigm for the use of space; a paradigm that blurs the traditional divide between civilian and military uses. Accordingly, the chapter by Ntorina Antoni explains how the definitional approach used across the chapters of this book can be stated as: “Space security” is the aggregate of all technical, regulatory and political means that aims to achieve unhindered access and use of outer space from any interference as well as aims to use space for achieving security on Earth. This adds to an already existing abundance of definitions for space security. Since it is not likely a consensus can be reached, the definition for the *Handbook of Space Security* maintains the practice of attempting to narrow general applicability and tailor definitions to specific uses. This definition serves as a frame for the focus and the structure of the Handbook.

Governance and theoretical perspectives form other foundational aspects of space security. Effective governance is needed for humanity to derive more benefits from space; space governance also seeks to ensure space is used in stable and sustainable ways. The challenges to international space governance in ensuring space as a safer and more secure environment are enormous. These include the increasing number of actors, growing commercialization, expanding military space programs, the proliferation of anti-satellite weapons, and lack of consensus among states on the need for and realization of a conclusive and universally negotiated treaty to prohibit an arms race in space. Ahmad Khan and Sufian Ullah indicate that any model for space governance should aim to reconcile the inherent competitive tendencies among states by incentivizing further cooperation. The idea of effective global space governance should seek to maximize the prospects for peaceful exploitation of space as a *global commons* by encouraging responsible behavior of states. My chapter asserts that spacepower theory can describe, explain, and predict how individuals, groups, and states can best derive utility, balance investments, and reduce risks in their interactions with the cosmos. Such foundational theory should be more fully developed and become a source for critical insights on finding better ways to generate wealth in space, making trade-offs between space investments and other important goals, reordering terrestrial security dynamics as space becomes increasingly militarized and potentially weaponized, and seizing exploration and survival opportunities that only space can provide.

Chapters exploring the laws of war for space and the role of space in deterrence complete the foundational part of Part 1. Steven Freeland and Elise Gruttner explain how the regulation of space is embedded in international law and explicate the major themes of the 1967 Outer Space Treaty (OST), the main source of space law. As technology advances, space has been increasingly used during the course of armed conflict, notwithstanding the “peaceful purposes” provisions of the OST. Reconciling these seemingly incompatible concepts and developments is difficult and requires an understanding of how and to what extent the international law principles of *jus in bello* – body of legal norms that regulate the conduct of participants in armed conflict – as well as international humanitarian law, apply to the conduct of these activities. Freeland describes how the rising number of “dual-use” satellites

further complicates matters and asserts that there is a growing need to reach consensus on additional legal regulation for armed conflict that may involve use of space capabilities. Stacey Henderson's chapter about Arms Control stresses that the current international law regime applicable to outer space does not prohibit the placement or use of all weapons in outer space, prohibiting only nuclear weapons and weapons of mass destruction, and is not capable of preventing a conventional arms race in outer space.

John Klein and Nickolas Boensch assert that even though deterrence has a legitimate role in future space strategy, it is not the panacea for preventing conflict. History shows that deterrence will at times fail due to miscalculation, uncertainty, or chance. They conclude that the enduring nature of war and strategy (and therefore deterrence) as well as the evolving character of war, indicate that the implementation of space deterrence should also be expected to change. This change is currently reflected by the growth of the commercial space sector (particularly in the United States, Europe, China, and Japan) – whether in reusable or responsive launch vehicles or mega-constellations of Earth imaging and communications satellites. In view of the increasing complexity of the space environment, resilience has emerged as a pervasive concept in contemporary space security. Regina Peldszus analyzes resilience from two distinct but complementary approaches: mission assurance and deterrence as well as high reliability and resilience engineering. Drawing on contemporary thinking from civilian and military perspectives, resilience is addressed as a distinct yet malleable notion at the intersection of space security and safety. She concludes that resilience is likely to continue as a key concept in space policy and systems planning. Straddling the fields of space security and reliability, it may inform, enrich, or even galvanize the more traditional security and safety management disciplines.

---

## **International Space Security Focus Areas**

Maintaining the ability of this domain to support safe, sustainable, and secure access and use for all – the essence of space security – requires cooperation. Jessica West explains that although cooperation is embedded as a core value within the institutions and laws that govern outer space, new uses and users of outer space are changing the dynamics of space security cooperation. This means that while cooperation can enhance security in space for those involved, it may come at cost to the long-term security of space by increasing strategic rivalry and facilitating the escalation of conflict into outer space. Jana Robinson and co-authors address the China's and Russia's global space footprint in the economic and financial (E&F) domain. They describe how the pace and nature of these international space partnerships concluded by China and Russia present a strategic and competitive challenge for Europe, the U. S., and other allies, including the development of global space governance, as well as markets based on transparency, good governance, and disclosure. The authors assert that the more subtle strategy deployed in the developed, democratic countries, to gain influence is conducted on an incremental basis, while the other approach, described as



“space sector capture,” mostly involves developing countries and consists of offering package deals of capabilities, services, and financing, creating sole-source supplier relationship and long-term dependencies.

Ulrike Bohlmann and Gina Petrovici explain how the Cold War drove both innovation in space technology and imposition of controls on the export of these technologies. Balancing national security and commercial interests has been and remains difficult due to the Janus-faced, “dual-use” nature of space technology, serving scientific and commercial interests on the one hand and strategic, defense-related objectives on the other. Export restrictions play a significant role within the sovereignty of a state, assert Annamaria Nassisi and Isabella Patatti, and therefore keeping the technological edge is perceived as a form of dominant power. As the demand for space-based security is very high, major spacepowers are inclined to protect critical technology, rather than exporting it. Alexandru Georgescu highlights that space systems are a key enabler for a wide variety of applications which have become critical to the functioning of modern societies. He uses the Critical Infrastructure Protection framework to argue that space systems may constitute a new form of Critical Infrastructure, dubbed Critical Space Infrastructure, and traces the positive impact that such a perspective may have on space security governance.

With regard to cybersecurity, Stefano Zatti asserts that the security measures implemented in space-based systems may turn out to be insufficient to guarantee information assurance against possible cyberattacks. Accordingly, security-specific aspects of the European Space Agency’s (ESA) space missions, along with specific cyber threats and possible countermeasures are addressed. Space safety is necessary for the sustainable development of space yet, as Joe Pelton and his coauthors describe, safety considerations are too often an afterthought for space security issues. Without improved space safety practices and standards from launch, to on-orbit operations, to reentry, billions of dollars of space assets, many astronaut lives, and even people on Earth could all be increasingly in peril. A related topic of growing importance is the concept of space traffic management. William Ailor’s chapter begins by providing an overview of the evolution of the near-Earth space environment, discussing the current situation, and projecting how the addition of large constellations of satellites to low-Earth orbit (LEO) will affect that environment. Just as the growth in air travel led to air traffic management, assuring that future space systems will have minimal interference to their operations requires a system to warn operators of potential collisions and other hazards: a space traffic management system.

Space sustainability is a concept that has emerged within the past 15 years to refer to a set of concerns relating to outer space as an environment for carrying out space activities safely and without interference, as well as to concerns about ensuring continuity of the benefits derived on Earth from the conduct of such space activities. Peter Martinez, as a long-time international space policy expert, is in an ideal position to review the role of the various relevant United Nations (UN) entities in ensuring space sustainability and provide a detailed review of the Working Group on the Long-Term Sustainability of Outer Space Activities within the Scientific and Technical Subcommittee of the United Nations Committee on the Peaceful Uses of

Outer Space (UN COPUOS). In addition, his chapter discusses the relationship of the work in UN COPUOS with related work being done in the Conference on Disarmament, the UN Group of Governmental Experts (GGE) on Transparency- and Confidence-Building Measures (TCBMs) in Outer Space Activities, and the initiative by the European Union to propose a draft international Code of Conduct for outer space activities. Finally, George Kyriakopoulos addresses space security as part of the overall international security, the maintenance of which constitutes the fundamental purpose of the UN Charter. In particular, he asserts that preserving security with respect to the celestial bodies requires the activation of mechanisms able to guarantee that the existing *status quo* will not be compromised by the placement of offensive weapons on them or potential conflict over the exploitation of space resources.

---

## Conclusions

This overview of Part 1 of the second edition of the *Handbook of Space Security* provides a comprehensive introduction to major issues and themes that shape humanity's dialogue about space security. The 17 chapters in Part 1 include foundational discussions about definitional, governance, theoretical, legal, deterrence, and resilience themes for space security as well as more focused discussions about cooperation, strategic competition, export controls, critical infrastructure, cyber threats, safety, traffic management, and sustainability. These chapters provide a comprehensive foundation for the more detailed and focused discussions of space security themes and issues in the remainder of the *Handbook of Space Security*.



# Definition and Status of Space Security

# 2

Ntorina Antoni

## Contents

Introduction .....	10
Definition of Space Security .....	11
Security Definition .....	12
Space Security Evolution .....	13
Space Security Definition .....	15
Status of Space Security .....	16
Africa .....	16
Asia-Pacific .....	18
Europe .....	21
The Middle East .....	23
Latin America .....	25
North America .....	26
Russia .....	28
Key Priorities .....	29
Concluding Remarks: The Way Forward for Space Security .....	30
References .....	31

## Abstract

Space security has gained increasing importance over the past decade as space becomes part of our everyday life. Yet, space security is not universally defined. The shift of paradigm and transformation of the space domain through new ways of utilizing space and recent technological advances such as mega-constellations, 5G, Internet of Things, artificial intelligence, and advanced materials have resulted both in major challenges and new opportunities. Over the years, space security has evolved. Since the signature of the Outer Space Treaty in 1967, space security has become a complex, broader, and multilayered concept. The topic dominates space

---

N. Antoni (✉)  
Eindhoven University of Technology, Eindhoven, The Netherlands  
e-mail: [ntorina.antoni@gmail.com](mailto:ntorina.antoni@gmail.com)

law and space policy agendas at the United Nations General Assembly Committees and the Committee on the Peaceful Uses of Outer Space along with its subsidiary bodies. In this context, this chapter aims to effectively capture the multifaceted concept of space security and provide an overview of its current status.

---

## Introduction

Space security entails the possibility to access and use space for all nations. Although traditionally it has been associated with military engagement, over the past years it has been enriched with safety aspects. The space race between the United States and the former Soviet Union in the 1960s triggered the first concerns regarding space security. The attempt to end an arms race in space was effected with the conclusion of the United Nations (UN) Outer Space Treaty in 1967 (United Nations 1967). The treaty sought to define boundaries for the security of outer space by establishing the principle of peaceful purposes in accordance with the UN Charter and by prohibiting the militarization and weaponization of space. The ratification of the Outer Space Treaty was a remarkable endeavor of resolving the space race tension, ensuring stability, and promoting international cooperation. Thus, space security – although not explicitly defined – was the result of the stabilizing effect of a treaty-based mechanism, and *vice versa* space security meant that activities in outer space ensure stability and peaceful uses of outer space (United Nations 1967). In this context, the interrelatedness between space security and stability was reinforced by the explicit distinction between civil and military uses of outer space.

Five decades later, the scope of space security has changed. As Sheehan notes in the chapter “Defining Space Security,” of the previous edition of this Handbook, “space security includes now aside the military dimension, also, economic, societal and environmental dimensions” (Sheehan 2015). These elements are indispensable to space security, in view of the ongoing transformation of the space sector that moves away from the traditional confines of space activities. The so-called New Space encapsulates major changes taking place at unprecedented rate. These are related to the growing participation of private actors, the rising number of space-faring nations, and the emergence of the civil-military paradigm. This means that the dividing line between civilian and military uses of outer space has yet become artificial leading to uncertainty regarding governance of dual-use or hybrid areas. The terms “safety,” “security,” and “defense” are intertwined and used interchangeably with no clear separation between areas of action. In many languages there is no clear distinction between the words safety and security. The cultural aspects of safety, security, and defense vary from country to country and from region to region. What is more, the understanding of space security has been redefined considering the new often blurred borders between safety – a clearly civilian area – and defense – a clearly military one. Security lies in between and for some countries/regions is closer to safety while for others closer to defense. This debate extends to governance questions as to who has legitimacy to act in space security and for what type of actions. Also, what would the role of the civil and defense actors respectively be and

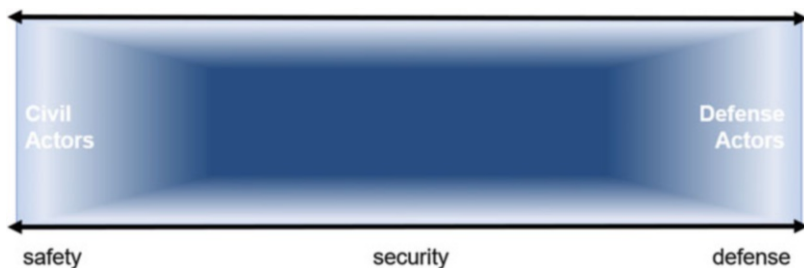
in which area. Accordingly, the various and divergent concepts, approaches, and definitions across the chapters of this Handbook are representative of an evolving space security landscape.

The absence of an internationally agreed definition – combined with the systemic nature of the space sector with multiple strategic objectives – presents challenges when endeavoring to build cooperative approaches among diverse organizational actors. As such, this requires the development of a mechanism that fosters new forms of cooperation among states in the advent of the new space era. Therefore, stability remains of strategic importance to the space sector, as it influences the effectiveness of states to manage the growing challenges and ultimately ensure space security. Accordingly, the remainder of this chapter will address definitional aspects and the current status of space security. It will provide an overview of space security perspectives in Africa, the Asia-Pacific, Europe, the Middle East, Latin-America, North America, and Russia. Such an approach will help to identify the underlying challenges related to space security and advance the understanding of the civil-military paradigm therein. The latter is a main challenge that needs to be taken into consideration for the development of space security enhancing mechanisms.

---

## Definition of Space Security

There is no commonly agreed definition and uniform understanding of space security. Be that as it may, there are myriad definitions adopting either a “soft” or “hard” approach. Often, the concept of “security” is used instead of the term “safety” or the term “defense,” or instead of both. This creates ambiguity concerning the content of space security and the set of underlying shared values and principles. As a result, the lack of clear boundaries between these concepts poses a major definitional challenge for space security, as depicted in Fig. 1. In attempt to address this definitional challenge, this section will first take a closer look into the security concept under international relations/law perspective and, then, it will examine the evolution of the security concept in the outer space context.



**Fig. 1** Definitional challenge for space security

## Security Definition

*Security* is derived from the Latin term *se + cura*, meaning free from care. Security means the quality or state of being secure, such as freedom from danger (safety) and something that secures protection. International relations scholarship has not agreed on a single definition of space security, due to its contested nature in the post-Cold War era as well as its overall subjectivity. In the words of Gallie (1956) security is often referred to as an “essentially contested concept” one for which, by definition, there can be no consensus as to its meaning (Williams 2013). According to Williams, “security is most commonly associated with the alleviation of threats to cherished values; especially those which, left unchecked, threaten the survival of a particular referent object in the near future” (Williams 2013). Maintaining international peace and security is the central mission of the UN as per Preamble of the United Nations Charter. As such, the UN has agreed to: “take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace” (United Nations Charter, Article 1). Thus, although security is not defined under international law, it is perceived as closely influenced by the concept “peace” and “peaceful means.”

The lack of clear definition has led to the interpretation of security from several perspectives, namely, individual, national, international, and global (McDonald and Brollowski 2011). Over time, security became intertwined with the concepts of territoriality and sovereignty of states, as reflected in the term “national security” and “defense.” *Defense* is derived from the Latin term *defensum* meaning “thing protected or forbidden.” In the broad sense it means “the act or action of defending.” Defense pertains to the protection of states’ territory, including its property and population, via diplomatic channels or by use of force (McDonald and Brollowski 2011). The use of force is stipulated in Article 2, paragraph 4 of the UN Charter while the right of a State to use force in self-defense is long-established in customary international law (Greenwood 2011). Provided that no definition of defense is provided, the main understanding of national security and defense in this context is interrelated with political and military security used by states (McDonald and Brollowski 2011).

Although the traditional concern has been related to security from external military threats and the use of force, the notion of security has evolved to include additional threats to a number of values: environmental security, economic security, physical security, human security, etc. (Baldwin 1997). In 1995, the United Nations Secretary-General called for a “conceptual breakthrough” of security which goes beyond the confines of “armed territorial security” to include also “the security of people in their homes, jobs and communities” (Rothschild 1995). This shifts the focus of security from states to people. This type of security stands closer to the notion of “safety” which is related to the human right perspective of security or the security of the individual as stated in Article 3 – right to life – of the UN

Universal Declaration of Human Rights. *Safety* is derived from the Latin term *salvus* meaning “uninjured, in good health.” Safety means “the condition of being safe from undergoing or causing hurt, injury, or loss” and “something that secures protection.” Accordingly, this notion of security – mainly associated with safety – has gained attention by international relations scholars as well as the UN, who seek to give a broader interpretation to security that includes economic, food, health, environmental, personal, community, and political security (Baldwin 1997; Osisanya 2015).

## Space Security Evolution

The definition of space security is as elusive as the definition of security itself. Similarly, to the ambiguity of the security concept within the frame of international relations, there is no universally agreed definition on space security. As such space security is a multifaceted term that many have attempted to define yet no consensus has been reached. The evolution of the security concept over time combined with the evolution of outer space activities poses unique challenges to the understanding and definition of space security. What is more, a significant challenge remains the dual-use nature of space technology and applications.

The military perspective of space security, closer to the “defense” side, has to a large extent derived from the global agenda on international peace and security. The launch of Sputnik-1 in the 1960s, followed by the first manned spaceflights in the 1970s, marked a technological race between the former Soviet Union and the United States. This created the fear of an arms race in space and profoundly influenced the definition of space security. In this regard, the international community was concerned that space could be used for military purposes. Accordingly, the UN General Assembly adopted in 1958 the Resolution 1348 (XIII) “Question of the peaceful use of outer space,” where it expressed the desire to “avoid the extension of rivalries into this new field.” The principles set forth in this resolution combined with those of the subsequent resolutions (1961 and 1962) were ultimately embodied in the UN Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies, with the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) being the most important UN body engaging in the development of international space law (United Nations 1967).

The Outer Space Treaty establishes outer space as a *global commons*, not subject to national appropriation. The States Parties to the treaty recognized that it was in the common interest of all mankind to commit to broad international cooperation in the scientific as well as the legal aspects of the exploration and use of outer space for peaceful purposes. The 1996 UNGA Declaration on International Cooperation further elaborates on the modes of cooperation that are considered most effective and appropriate “including, inter alia, governmental and nongovernmental; commercial and non-commercial; global, multilateral, regional or bilateral and international cooperation among countries in all levels of development.” In addition, the treaty makes explicit reference to the applicability of international law and the UN Charter

to outer space. Article III stipulates that: “States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the moon and other celestial bodies, **in accordance with international law**, including the Charter of the United Nations, in the interest of **maintaining international peace and security** and promoting international co-operation and understanding” (bold by the authors). Furthermore, Article IV paragraph 1 prohibits the placement in orbit around the earth of “any objects carrying nuclear weapons or any other kinds of weapons of mass destruction,” and it adds that “The moon and other celestial bodies shall be used by all States Parties to the Treaty **exclusively for peaceful purposes**. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manoeuvres on celestial bodies shall be forbidden. The use of military personnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration of the moon and other celestial bodies shall also not be prohibited” (bold by the authors). Despite the premise of peaceful purposes, the explicit prohibition of the weaponization and militarization of outer space, and the application of international law, the boundaries of space security under the body of international space law remain yet dubious.

However, the distinction between civilian and military uses of outer space is not easy to draw due to the strong dual-use nature of space technology. From a technical point of view it is not easy to tell whether certain space technologies in the fields of satellite communications, positioning, navigation and timing, and space situational awareness are used for civilian applications and programs or for military and defense purposes. The dual-use factor is the main reason that the United Nations Group of Governmental Experts (GGE), aiming at exploring legal instruments that prevent the placement of weapons in outer space, failed to reach a consensus on a substantive report in October 2019. During the General Assembly’s First Committee on discussing related draft resolutions one of the delegates stated that “Due to the dual-use nature of space objects, it is inherently difficult to define an outer space weapon or to know and verify intentions behind certain related activities.” Another one highlighted “the current blurred distinction between civil, commercial and military activities in outer space, saying the international community must bring new ideas to discussions going forward” (United Nations 2019). This blurred dividing line between civilian and military applications is further exacerbated by the increasing commercialization of outer space and the new security paradigm of hybrid threats that are also applicable to outer space. On the one hand, the growing commercial sector enables the pursuit of military authorities to modernize space capabilities. Such a trend is reflected in a recently commissioned study to explore the possibilities and risks of employing commercial systems for the proposed US Space Force (SpaceNews 2020). On the other hand, the availability of civilian or commercial space assets to security- and defense-related missions contribute to the proliferation of hybrid threats to space. These include active operations, such as cyberattacks, jamming or spoofing, dazzling, and passive ones such as hiding or moving assets (Robinson 2018).



What is more, the increasing participation of private commercial actors in space security has raised some concerns related to the “softer” side of space security, namely space safety and sustainability of outer space activities. Space safety regards the use of space technology and applications with societal benefits, namely, water management, marine and coastal ecosystems, health care, climate change, disaster risk reduction and emergency response, energy, navigation, seismic monitoring, natural resource management, biodiversity, agriculture, and food security. Hence, space safety extends to the security of space systems in order to provide for security on Earth, as well as for space sustainability (► [Chap. 15, “Space Safety”](#)). In February 2018, at the 55th session of the UN COPUOS – Scientific and Technical Subcommittee, agreement was reached on nine additional guidelines on the long-term sustainability of the outer space activities, with the following definition: “The long-term sustainability of outer space activities is defined as the ability to maintain the conduct of space activities indefinitely into the future in a manner that realizes the objectives of equitable access to the benefits of the exploration and use of outer space for peaceful purposes, in order to meet the needs of the present generations while preserving the outer space environment for future generations” (► [Chap. 17, “Space Sustainability”](#)).

## Space Security Definition

Based on the above, the different perspectives of space security have led to myriad definitions. For instance, the Space Security Index (SSI) defines space security as “the secure and sustainable access to, and use of, space and; the freedom from space-based threats” (Sheehan 2015). Another example is that the European Union defines space security as “security from space, where Space-based assets and systems are critical to ensuring security on Earth, and security of space, where these assets need to be protected in the difficult environment of outer space.” Since it will be difficult to reach consensus among states, and any definition might end up being obsolete provided the rapid transformation of outer space activities, it is imperative to narrow general applicability and tailor-made approaches. To that end, the following definition is provided in this Handbook:

“Space security” is the aggregate of all technical, regulatory and political means that aims to achieve unhindered access and use of outer space from any interference as well as aims to use space for achieving security on Earth.

This approach helps to structure the myriads of definitions and cover the full spectrum of constitutive elements thereof. Such a definition is thus necessary to reach a common understanding and support cooperative and collective frameworks in order to tackle the inherent complexities of space security in a constantly shifting environment. A foundational challenge arising from space security initiatives at the national, regional, and intergovernmental levels is the need for collaboration and

synergies between civilian and military entities as depicted in Fig. 1. Such a challenge leads to uncertainty in governance, strategy, and policymaking aspects of space and security. In this regard, considerations need to be made for mechanisms that can effectively deal therewith and ensure stability and international cooperation for space security.

---

## Status of Space Security

The new paradigm shift in space security has influenced the expectations of countries and regions around the world. This part will address the status of space security in order to identify strategic priorities and needs on space security.

### Africa

Space activities in Africa have been increasing over the past decades, with different countries having reached different levels of investment and development. African actors include organizations that operate at the continental level, such as the African Union (AU), regional organizations, typically the Regional Economic Communities (RECs), technical organizations such as specialized agencies and institutes in different areas and the African space agencies (Giannopapa 2011).

Space security engagement in African countries is more visible on the civil side, in particular regarding the benefits that space can bring to Earth. African countries that engage on space can be split into three main categories: passive users, active users, and active developers. Passive users are African countries that do not have any space capabilities. They only receive information already processed by others. Active users are African countries that have the capacity to process the information offered. Active developers are those African countries that themselves have capacity in space activities and typically have also a space agency and more advanced space policy provisions, either contained in self-standing documents or as parts of other policies. Space security is perceived according to the user needs of the countries. Most considerations are related to the use of space security for societal purposes on Earth. Space applications can assist in providing solutions to people's basic needs such as providing food and water security, health care, education, early warning, disaster management, and emergency response. Nevertheless, the benefits of space applications are not sufficiently communicated to decision makers or the wider population, and there is not enough basic education at various levels to perform, manage, and operate space-based assets. Various space projects in different areas have been developed in Africa but very few are sustainable beyond the pilot phase. This is because often the local community of end users is not involved from the beginning and does not have a feeling of ownership. Appropriate bodies have not been identified within the government structure to take up the responsibility for running and maintaining the project. The projects developed in Africa are typically conceived by developed countries, which have not properly captured the societal

needs and infrastructure restrictions of the underdeveloped countries they purport to be helping (Giannopapa 2011).

African countries have been looking into the European model for regional cooperation on space activities with the African Union taking the lead, while countries that are active developers engaging in bilateral cooperation with global players. The 2017 African Space Strategy, which sets out the objectives for an African Space Program, is mainly focused on scientific and public good applications (African Union 2017). The strategy was adopted by the African Union heads of states and government, representing 55 member states on the African continent. According to the policy, satellites are enabling tools aimed to tackle challenges in Africa, including water resources, weather monitoring, security assistance in conflict zones, disaster aid planning, infrastructures, and food security. The focus is predominantly on space security for Earth. Food security enabled by space systems is further elaborated in ► Chap. 40, “Space-Enabled Systems for Food Security in Africa”. The African Union has emphasized the importance of security and defense to the development of Africa (African Union 2015). As such, strategic priorities for the African Space Program focus on earth observation, satellite communication, autonomy and space science, navigation and positioning (UNOOSA 2019). Aside the civil use of space applications, the African Space Strategy outlines that earth observation data are important for military applications “where terrain profiling and mapping is critical for the deployment of ground troops, especially in hostile and remote territories” (African Union 2017). For example, at the national level, the 2018 South Africa National Space Strategy takes into consideration the dual-use of space activities and the interconnectedness of civil and military applications (Republic of South Africa 2018). However, no explicit reference is made in either document regarding the cooperation between civil and military authorities and the potential challenges of discrepancies between the regional and national levels.

Acknowledging the importance of coordinating the African space program, Egypt has been assigned to host the African Space Agency (African Union 2017). Yet, establishing the space agency has encountered many challenges due to governance issues and financial implications. In order to realize these objectives, the African Union convenes regular annual space conferences with African space actors as well as UN representatives, academia, and the private sector (African Union 2020). This inclusive approach is necessary provided the increasing number of countries that have national space programs. While South Africa has established links for space security cooperation at the bilateral and multilateral levels and is also finalizing a new space legislation (Lal et al. 2018), other countries in Africa are lagging. Accordingly, the next steps are focused on mobilizing resources across all African countries to facilitate the launching and implementation of the African Space Agency (African Union 2020). These steps are necessary in order to overcome the political fragmentation and improve the governance of the African space program. It is thus fundamental to form a coordinated regional approach for the development of space activities, which can also tackle safety and security challenges in the continent. Such approach can further facilitate the representation of Africa at the international cooperation *fora* and enhance international cooperation.

## Asia-Pacific

Independent space powers coexist in Asia, namely Japan, China, India, South Korea, Pakistan, and Australia. Asia is the world's second-largest defense spender while it is becoming increasingly active in space. The geopolitical and military competition in Asia has an impact on the space efforts of these countries (► [Chap. 27, "Space Security in the Asia-Pacific"](#)). There are three key drivers to space in Asia: increasing use of space for military purposes; civilian use that could also lead to conflict because of congestion and competition; and investments in military technologies such as those for anti-satellite (ASAT) tests and missile defense. The growing space competition is demonstrated by the rapidly growing development of counterspace capabilities, such as kinetic ASAT missiles, electronic and cyber warfare capabilities, and new efforts at creating specialized military agencies devoted to space utilization. The Asia-Pacific Space Cooperation Organization (APSCO) is an intergovernmental space cooperation organization headquartered in Beijing, China, and its members include China, Bangladesh, Iran, Mongolia, Pakistan, Peru, Thailand, and Turkey. It was founded in 2005. Both Japan and China have been trying to set up regional cooperation under their respective leadership, resulting in two different formats for governance. While Japan established an Asia-Pacific Regional Space Agency Forum (APRSAF) in 1993, China founded the APSCO in 2008. Membership is somewhat overlapping, with institutions from 40 states (including non-Asian) participating in APRSAF, and 8 formal member-states in APSCO. This indicates the basic difference between the two: APRSAF is a coordination mechanism of institutions (space agencies, research establishments, space applications users, etc.), while APSCO is an intergovernmental organization.

*China*, over the past decades, has been rising as one of the major space powers worldwide toward establishing dominance. In a stepwise approach, it has set out its ambitions and a long-term strategic and programmatic development. Among other achievements, the landing of an unmanned mission on the near side of the Moon using its Chang'e 3 in December 2013 and the Chang'e 4 landing on the far side of the lunar surface in January 2019 have marked China's presence as an international space power. The engagement has been increasing on the civil side using space to provide space security on Earth, while information and communication technologies have gained impetus in overall national power and especially military capability (► [Chap. 29, "Chinese Concepts of Space Security: Under the New Circumstances"](#)). Many of China's satellites are dual-use, supporting urban planners and agricultural programs as well as the military. China's military-dominated and government-monopolized characteristics of space affairs aim to internationalize and commercialize the space industry (Nie 2020). Under the Belt and Road Initiative – expanding from China and Asia to Europe and Africa – China has been actively engaging in the Space Information Corridor project. The latter "takes communication, remote sensing, navigation satellites as the main body, with space-based information resources and ground information sharing network and aims at realizing co-construction and sharing of space information in the region" (Jiang 2019). Simultaneously, the emerging rise and engagement of China in the commercial

market will increase competition among other Asian states as well as with other countries. On the defense side, the relationship of space and national security has been evolving as part of a broader ongoing assessment of the role of information in future warfare (► [Chap. 29, “Chinese Concepts of Space Security: Under the New Circumstances”](#)). In 2015, China established the People’s Liberation Army’s (PLA) Strategic Support Force which saw the integration of the PLA space, cyber, and electronic warfare capabilities, which is considered a significant achievement considering the future of warfare that would see the interface between all these different capabilities. Due to the PLA’s attention to information and communications technologies, the centrality of space dominance has grown as well. As with other Chinese military activities, the PLA’s approach to space operates within the context of guiding thoughts. The guiding thoughts for space are “active defense, all-aspects unified, key point is establishing space dominance” (► [Chap. 29, “Chinese Concepts of Space Security: Under the New Circumstances”](#)).

*Japan’s* space policy has been influenced significantly by its overall foreign and security policy. At the start of its space activities, Japan was reluctant to engage in security-related uses of space, largely due to its pacifist constitution, which is interpreted to prohibit using space for security purposes. The Basic Space Law 2008 urged the government to use space systems “to ensure international peace and security and also to contribute to the nation’s security” (► [Chap. 30, “Historical Evolution of Japanese Space Security Policy”](#)). This has been evolving over the past few years. The country updated in 2013 its Basic Space Plan. The latter aimed at creating new opportunities for the involvement of Japan in international efforts to address the most pressing space security-related challenges of the twenty-first century. As such, this update and its subsequent revision in 2015 marked the reorientation of Japan’s space program toward tackling the changes in its surrounding security environment. The latest document reflects the new national security policy 2014 (military use of space) and establishes long-term and concrete public investment plan for the upcoming 10 years (Komiya 2016). In particular, the latest version of the Basic Space Plan aims at responding to the growing threat of ASAT weapons and the increasing quantity of space debris by putting emphasis on space security, through strengthening security capabilities and the Japan-US alliance and ensuring the stable utilization of outer space. The two key projects envisaged in the new plan are the development of a Space Situational Awareness (SSA) system with ground and space segments, and the establishment of self-defense forces. In addition, Japan is preparing a new series of Earth observation satellites to tackle natural disasters and limited natural resources. Accordingly, a new space security budget is developed with contributions of Japan Aerospace Exploration Agency (JAXA) and the Ministry of Defence (Euroconsult 2019). Therefore, the revised Basic Plan represents a completely new direction of Japanese space policy with increasing role for the military. On April 19, 2019, the United States and Japan reiterated their commitment to military space activities and highlighted that space, cyberspace, and the electromagnetic spectrum are priority areas to better prepare for cross-domain operations (Spacewatch.global 2019).

*India* over the past year has also been rising to a world space power. It has acquired multifaceted space capabilities with dual-use applications – both civilian and military – and focuses on achieving autonomy in space including launchers, satellite communications, Earth observation, and navigation. Overall, India has followed the policy of the use of space for socioeconomic development. Over the years, the Indian Space Research Organisation (ISRO)’s program has matured significantly, and, at present, Indian space program is regarded as one of the important space programs in the world. From launching small satellites to undertaking successful missions to the Moon and Mars, India has excelled in almost all areas of space experimentations (► [Chap. 31, “India in Space: A Strategic Overview”](#)). Additionally, India has made significant investments toward establishing its military architecture owing to its strategic needs. Space technologies have become central to strengthening this architecture, essentially as a force multiplier. The March 2019 ASAT test clearly communicated India’s intention and capability to use space for military purposes. Soon after the test, India has announced plans to establish a Defence Space Agency along with a Defence Cyber Agency marking a shift in the evolution of the Indian space strategy (Euroconsult 2019). The launch program remains one of India’s main objectives to ensure independent access to space. Starting with the development of the Satellite Launch Vehicle (SLV-3) during the 1970s, it has progressed through the Augmented Satellite Launch Vehicle (ASLV), Polar Satellite Launch Vehicle (PSLV), and Geosynchronous Satellite Launch Vehicle (GSLV). Recently, the development of the next-generation launch vehicle, the Geosynchronous Satellite Launch Vehicle Mark III (GSLV MkIII), has been completed and has become operational. India’s next milestone mission of Human Spaceflight has been initiated, and the first crewed flight is expected by 2022 (► [Chap. 70, “Indian Space Program: Evolution, Dimensions, and Initiatives”](#)).

The space sector in *Australia* is experiencing an unprecedented level of public interest and government support. National security considerations and the economic benefits of a fast-growing world market for space products and services are inextricably linked as drivers for a range of government and industry initiatives (► [Chap. 71, “Australia’s Space Security Program”](#)). The Government’s clear intention is to enhance Australian Defence sovereign space capabilities progressively through dedicated Intelligence, Surveillance, Reconnaissance (ISR); space and cyber programs; SSA systems; and military satellite capability (Euroconsult 2019). In May 2016 the Australian Department of Defence announced that it is preparing a roadmap for a \$2.3 billion next-generation satellite communications investment on mixing commercial and military capability. Australia is now treating space as an integral component of its role in the protection of its national security interests and in the advancement of its international responsibilities. In September 2017, the Australian Space Agency was established to take over the operational and regulatory activities. Regarding the development of space policy, the 2017 Space Industry Association of Australia (SIAA) White Paper suggests that ensuring long-term access to space, for strategic purposes requires both civil and military capabilities. Along the same line, the Australian Civil Space Strategy 2019–2028 focuses on seven national priorities: position, navigation, and timing; earth observation; communication technologies,

and services; “leapfrog” research and development; space situational awareness; robotics and automation; and access to space (► Chap. 71, “Australia’s Space Security Program”).

*South Korea* is implementing a pro-active space program in order to create autonomous operational capabilities in areas such as Earth Observation, as well as to develop domestic industrial capabilities for satellites and launch vehicles, and to build the associated infrastructure. Space development in South Korea is driven by the National Space Development Promotion Basic Plan, with the third pillar including exploration and navigation as two key elements for 2018–2022. South Korea has historically focused on satellite development, while more recently expanding into space launch vehicles. Furthermore, South Korea is trying to meet national user needs, to serve external needs commercially, and to increase its participation in international programs. The next challenge for the country is to complete the development of the launcher KSLV-2 (Euroconsult 2019).

*Pakistan*, despite political, technological, and economic constraints, is considered an aspiring space power, although with a relatively modest space program compared to the larger, more successful ones of China and India. The country aims to utilize available resources to improve its nascent space infrastructure through collaborative efforts to gain eventual self-sufficiency for socioeconomic and strategic purposes in the South Asian region (► Chap. 72, “Pakistan’s Space Activities”). The Space Development Program 2040 approved by the National Command Authority aims to ensure space-based benefits for the country and focuses mainly on telecommunications and Earth observation. In addition, Pakistan has close ties to China via the China-Pakistan Economic Corridor (CPEC). It considers a manned space mission in 2022. Yet, SUPARCO’s (Space and Upper Atmosphere Research Commission) lack of funding impedes technological advancement and innovation (Euroconsult 2019).

## Europe

In Europe, the space sector is a particularly interesting and dynamic field, mainly because Europe includes several space faring nations with varying capabilities and priorities. Due to the inherent dual-use nature of space activities, responsibility for space has traditionally resorted under a State’s sovereign competences. Traditionally, security- or defense-related space programs have been established and maintained at the national level or dealt with bilaterally or multilaterally in *ad hoc* cooperative programs. Only civilian space activities, including Earth observation, telecommunications, human spaceflight, space transportation science, and technology development, were the subject of cooperation at the regional and intergovernmental levels. However, the past years/decade the security dimension of space activities has increasingly been coming to the attention of European countries, as well as the European Union (EU) and the European Space Agency (ESA). “Space and security,” both in its security from space and security in space aspects, is progressively contributing to the further integration of space activities in sectorial policies (Giannopapa et al. 2018). Today, space security constitutes the second pillar of

activities of the ESA as agreed by the Ministers of ESA's Member States in November 2019. Additionally, the European Commission in its new organizational structure creates a dedicated Directorate General Defense Industry and Space, with the new president Ursula von der Leyen viewing it as one of the EU's priorities to reinforce the European defense capacities. This directorate aims to exploit the growing possibilities that space offers for the security of European citizens, including the capitalization of synergies between the civil and defense sectors.

Over the past several years, the EU has formulated a space security strategy, including in the 2018 Proposal for a Regulation for a Space Programme for the EU which is based on the 2016 Space Strategy for Europe. One of the main goals of the 2016 Space Strategy for Europe is to "Reinforce Europe's autonomy in accessing and using space in a secure and safe environment." The Regulation for a Space Programme proposes the development of Governmental Satellite Communications (GOVSATCOM) and SSA programs to accompany the satellite navigation program Galileo and the earth observation program Copernicus. The European family of launchers includes the Ariane 5, Vega, and Soyuz that secure Europe's independent access to space and are launched from the Guiana Space Centre. At the same time, ESA has more explicitly formulated its space security policy, as reflected in the "Elements of ESA's Policy on Space and Security" and the safety and security program adopted at the Ministerial Council in 2019. During the Ministerial Council 2019, ESA adopted a safety and security program and also secured the transition to the next generation of launchers: Ariane 6 and Vega-C, as well as the Space Rider, ESA's new reusable spaceship. European institutional programs are intertwined with the national and multilateral programs of the European countries based on their national budgets and contributions to organizations such as and the EU. In addition to ESA and the EU policy and programmatic developments, in 2019 NATO Defence Ministers approved its first ever space policy.

The different space security policies of the various European countries are to a large extent determined by national needs and priorities as brought forward through their participation in relevant space and security organizations, including ESA, EU, the European Defence Agency (EDA), and the North Atlantic Treaty Organization (NATO). The largest groups of European countries are currently members to all four organizations (ESA, EU, EDA, and NATO): Belgium, Czech Republic, France, Germany, Greece, Estonia, Hungary, Luxembourg, The Netherlands, Poland, Portugal, Romania, Spain, and the United Kingdom (due to Brexit the UK is no longer an EU Member State). A few countries belong to ESA, EU, and EDA, but they do not belong to NATO: Austria, Finland, Ireland, and Sweden. Norway is part of NATO and ESA. Even though Norway is not an EU Member State, it still participates in EU space programs and to EDA programs. Denmark is a NATO, EU, and ESA Member State but is not an EDA Member State. It also opted out of the EU Common Security and Defence Policy (CSDP). Slovenia is an EU and EDA Member State, and an ESA Associate Member State. Switzerland is an ESA Member State. Overall, the current priorities and trends in space and security are reflected on the space and security elements stipulated in national strategic documents. Depending on each European state, either a dedicated space security strategy is in place or space and security



aspects are included in strategy documents covering other policy areas. For example, space and security aspects can be found in maritime strategies and arctic strategies that also stress the importance of space-based assets and applications in these domains. The space activities and programs of European countries are centered on the fields of Earth observation, satellite communication, Global Navigation Satellite System (GNSS), SSA, space transportation, satellite operations, and detection, tracking, and warning. The institutional space and security policy developments in Europe have been developing in parallel with the policies of the European countries. All in all, European space and security governance is multifaceted, thereby posing a major challenge to effective cooperation among the EU, ESA, and the European States (► [Chap. 23, “Strategic Overview of European Space and Security Governance”](#)).

## The Middle East

The United Arab Emirates (UAE), Saudi Arabia, and Iran have emerged as regional leaders in the Middle East (Euroconsult 2019). In the recent years, Middle Eastern countries have come together to collaborate on satellite programs. Namely, in March 2019 the UAE Space Agency launched the Arab Space Coordination Group to build the first pan-Arab Earth Observation satellite via cooperation among its 11 member nations: Algeria, Bahrain, Egypt, Jordan, Kuwait, Lebanon, Morocco, Oman, Saudi Arabia, Sudan, and the UAE (National Defense 2020).

*The UAE*, a federation of six emirates with the world’s sixth largest oil reserves and the Middle East’s primary trading center, had essentially no involvement in space activities – other than shareholdings in communication satellites – until 2006, when the government of Dubai established the Emirates Institution for Advanced Science and Technology (EIAST). The latter was incorporated into Mohamed Bin Rashid Space Center (MBRSC) in 2015 which focuses on space research, satellite manufacturing, systems development, and Earth observation (Euroconsult 2019). In 2014, the UAE Space Agency was established with the mandate of overseeing and promoting the country’s space sector and activities. With this mandate the agency is responsible for the development of the so-called National Space Framework consisting of four main components, namely, Space Policy, Space Strategy, Space Law, and Space Regulations (► [Chap. 34, “UAE Approach to Space and Security”](#)). The UAE Space Agency actively cooperates with several international and regional space agencies such as those in the United States, France, China, India, Japan, South Korea, Italy, Germany, Kazakhstan, Bahrain, among others. The UAE is in the process of establishing its regulatory framework for space activities. In December 2019, the National Space law was approved and came into effect, hence setting the regulatory basis for space activities by covering the organization and objectives of space projects undertaken by the country, including peaceful space exploration and the safe use of space technologies. In the field of satellite communications, Al Yah Satellite aims to provide commercial, governmental, and military services, while at the same time focusing

on further growth, empowerment of human capital, and quality enhancement (► [Chap. 34, “UAE Approach to Space and Security”](#)).

*Israel's* space industry aims at achieving independence and national defense goals. The launch program – Shavit rocket – plays an important role in *Israel's* vision, making it one of the few nations with the ability to launch unmanned missions to space. The Shavit launch vehicle, operated by the Israel Defense Forces, was developed to enable *Israel* to launch its military reconnaissance satellites, the Ofeq series (Euroconsult 2019). In the past 30 years, *Israel* developed an indigenous space capability to develop, launch, operate, and maintain satellites in two main niche areas: Earth observation and communications, including the ground segment of communications satellites. *Israel's* focus continues to rely on a broad space infrastructure for defense and civilian applications under the auspices of the Ministry of Defence and the Israel Space Agency. The space agency aims at implementing a new space program, geared toward research and development while supporting multiple private and academic initiatives. In addition, the agency has forged bilateral cooperation with the United States and European countries (Euroconsult 2019). While security in the region has been *Israel's* key concern throughout its history, unsurprisingly security has also been the key driver of the country's space activities. It has, however, also resulted in the growth of the commercial space sector. *Israel* has expanded, in recent years, its cooperation with international partners, as well as established a civilian space policy backed by modest government funding. Within the context of protecting and encouraging this nationally important ecosystem, *Israel* considers international space security, safety, and sustainability to be of importance (► [Chap. 32, “Israel's Approach Towards Space Security and Sustainability”](#)).

*Iran* is a member of the Asia-Pacific Space Cooperation Organization (APSCO) since 2004 (Spacewatch.global 2016). *Iran* planned to build and launch satellites in 1996, but made little headway until 2004, when a broad review of plans and policies led to the creation of the Iranian Space Agency (ISA) and the allocation of a sizable budget under the sixth Five-Year Development Plan. ISA, which falls under the Ministry of Information and Communications Technology, along with the Ministry of Defence has cooperation agreements in place with Russia, Bolivia, Azerbaijan, and Kazakhstan. The Iranian space program is sustained by substantial research and development capabilities in its universities and defense industry, robust funding, and high-level political support. As such, the space program aims to fulfill both civilian and military objectives (Euroconsult 2019). The “Comprehensive Document of Aerospace Development,” which was adopted in 2012 and emphasizes the capabilities of *Iran* for space activities extending to both civilian and military entities. In February 2007, *Iran* tested a Sounding Rocket Vehicle (SRV) for research purposes which was followed by SRV 1. SRV 2, which was successfully launched into space, provided the opportunity for Safir SLV to launch the first national satellite, Omid (► [Chap. 33, “Policies and Programs of Iran's Space Activities”](#)). *Iran's* space program up to that point had been based on ground stations that relayed Intelsat communications and received Landsat data. In recent years, *Iran* has made steps in space science, space technologies, and space applications for civilian purposes mainly through communication satellites (Tarikhi 2015).

## Latin America

Currently, at the forefront of Latin America's space ambitions are two of Latin America's largest and most technologically advanced countries, Argentina and Brazil (Harding 2015). The Argentine National Space Activities Commission (CONAE) is responsible for Argentina's national civilian space activities, which are free from military control and entirely promote the peaceful uses of outer space. Its program is focused on Earth observation (Euroconsult 2019). In Chile and Peru, the current Earth observation satellite systems provide imagery for both military and civilian applications including disaster management (Euroconsult 2019). The Union of South American Nations (UNASUR) is an intergovernmental union established in 2008 (came into effect in 2011) to encompass all South American Countries. UNASUR previously discussed establishing a South American Space Agency; however, this has not yet been created (Sarli et al. 2018). In addition, the Space Conference of the Americas (CEA) is a continental forum of regional and international cooperation, created in the early 1990s by the United Nations General Assembly to achieve a convergence of positions on issues of common interest related to the peaceful use of outer space by its Member States. The objective is to agree on strategies to promote the practical use of space applications to support programs with a high degree of social content for the region, to encourage progress in and development of space law, and to strengthen educational programs and training in space science and technology (UNSPIDER 2010). Notwithstanding the value of these organizations, there is still no regional understanding or approach about space and security.

Despite the status to the economy in the region, *Brazil* has managed to sustain growth since the end of 2017 with an industrial production growing slowly. The Brazilian Space Agency (AEB), created in 1999, is responsible for the coordination of Brazilian space activities, with significant effort undertaken in Earth Observation and launcher development. AEB oversees implementing and coordinating Brazil's space policy in cooperation with the Ministry of Science, Technology, Innovations and Communication and the Ministry of Defense (Euroconsult 2019). National launching facilities were developed in Brazilian territory, including the Alcântara Launching Center (*Centro de Lançamento de Alcântara*), designed in 1983. Due to its geographic position, launchings benefit from the Earth's rotation in order to achieve greater speed, allowing fuel economy and increased payload capacity. Brazil's space-related objectives are described in the *Programa Nacional de Atividades Espaciais (PNAE) Planejamento 2012–2020*. The final segment of the Brazilian space program revolves around the development of a national launching vehicle, thus securing independent access to outer space. Named VLS (for Satellites Launching Vehicle, "*Veículo Lançador de Satélites*" in Portuguese), the program has faced budgetary and technical burdens since its conception operations (► Chap. 35, "[Space Security in Brazil](#)"). In 2012–2014, Brazil set out to indigenously develop a geostationary communications satellite, continued to support the joint China-Brazil Earth Resources Satellite (CBERS) program, developed two indigenously Brazilian space launch vehicles, supported its joint Brazil-Ukraine

Cyclone launch vehicle program referenced above, and established a science and technology research satellite program. Recently, the Brazilian Ministry of Defense signed, in December 12, 2018, a Space Situational Awareness agreement with US Department of Defense, as part of a larger effort to increase safety of space operations (► [Chap. 35, “Space Security in Brazil”](#)).

## North America

The *United States* remains the world’s leading space program, both when it comes to civil and defense space components. The space program has been further expanded by the Trump administration, for example through civil and defense budget increases, through policy and legislative initiatives, and through a proposed Space Force. In the United States, space policy has remained relatively consistent over the last 60 years with a focus on international cooperation, peaceful uses, and development of outer space for the common good. Throughout this time, the right of self-defense in space has been linked to military activity. Yet, the 2017 National Security Strategy made a notable shift regarding the security aspects, while at the same time the National Space Council was revived (► [Chap. 20, “War, Policy, and Spacepower: US Space Security Priorities”](#)). Accordingly, US Space Policy Directives 1 and 2 aim at fostering commercial activities through an appropriate regulatory framework, while Space Policy Directives 3 and 4 address the creation of space traffic management and the establishment of a space force respectively. The Space Policy Directive 1 calls for the United States “to lead an innovative and sustainable program of exploration with commercial and international partners,” while the Space Policy Directive 2 calls for the streamlining of regulations on commercial use of space. The Space Policy Directive 3 on Space Traffic Management (STM) aims for US leadership in space by stipulating the need to “set priorities for space situational awareness (SSA) and STM innovation in science and technology (S&T), incorporate national security considerations, encourage growth of the U.S. commercial space sector, establish an updated STM architecture, and promote space safety standards and best practices across the international community.” The Space Policy Directive 4 establishes the US Space Force as a sixth military branch of the United States Armed Forces within the Department of the Air Force.

Under the Space Policy Directive 3 responsibility for providing SSA data for civil use is assigned to the Department of Commerce (DoC), while the Department of Defense (DoD) will focus on maintaining access to and freedom of action in space. In particular, the Department of Commerce becomes the agency responsible for SSA data sharing and timely warning of collision avoidance, including conjunction assessments and maneuver plans, available to the public through the publicly available portion of DoD authoritative catalogue. The availability of the data is and will remain to be free of direct user fees. The Department of Defense, therefore, shifts the civilian part of its responsibilities to DoC and will oversee the military part of authoritative catalogue of space objects (U.S.FR 2018). Shall the Space Policy Directive 3 proposal be approved it does raise the following fundamental question:

first, how distinctive can the military SSA activities be from the civilian SSA activities and, second, will it be possible for them to integrate under one comprehensive regime? This has implications not only for the governance of the safety of operations and national security but also for the exchanges and coordination with other national and international organizations (Hitchens 2019). Managing STM ultimately boils down to balancing between to seemingly contradictory objectives; one being the safety and sustainability of outer space activities, and the other one being the national security concerns of the government as further depicted in the proposal for the creation of a space force.

Regarding space programs, the US military and intelligence organizations' programs combined constitute by far the world's largest space program. The services provided by these programs include telecommunications, surveillance, missile early warning, meteorology, positioning/timing, radio interception, nuclear detonation detection, and data relay. Space systems provide both tactical and strategic services to the US military and intelligence agencies and in some cases to those of its allies. Strategic functions include monitoring international security treaties, analyzing the security forces of current and potential adversaries, and providing information to the President and the Secretary of State. Tactical functions include supporting US military and intelligence forces around the world. Overall, the US military space program continues to dwarf (a) the military space programs of all other countries combined and (b) of US civilian agencies such as NASA. The USA is unique in deploying military satellites of all types and on a global basis, and there is little sign that this will change in the next decade (► Chap. 59, "Satellite Programs in the USA").

The *Canadian* new Space Strategy 2019 issued by the Ministry of Innovation, Science and Economic Development Canada recognizes the importance of space as "a strategic national asset which underpins everything from national security to the ability to connect Canadians living in rural and remote communities." Since 2016, the Ministry has committed to new investments worth over \$2.6 billion. Space systems are also considered vital to the Canadian Armed Forces, which rely on them to effectively conduct operations for the defense of Canada and North America and to contribute to global peace, safety, and security. One of the most important objectives of the strategy is Canada's future mission to the Moon by joining the US-led Lunar Gateway mission (Government of Canada 2019). The Canadian Space Agency (CSA) focuses on accelerating space business and modernizing investments through the Space Technology Development Program. The CSA also participates to the European Space Agency ARTES program. Concerning satellite communications, the Department of National Defense (DND) has ties with the United States in the context of the Wideband Global Satellite (WGS) System and the US Advanced Extremely High Frequency program with protected military satellite communications. The DND has also contributed to the Maritime Monitoring and Messaging Microsatellite in the field of automatic identification system (Euroconsult 2019). The DND and the Canadian Armed Forces are seeking to develop a common operating picture of space assets, based on the program Innovation for Defence Excellence and Security (IDEaS). As such, new space-based technologies will enable them to

maintain space situational awareness for informed, expedited decision making in support of space system operations (Government of Canada 2019).

## Russia

Outer space has become an important area for Russia which aims to rebuild its global status and prestige as a space power by intensifying the links between space and defense. Russia considers outer space predominantly as a strategic region to enhance its military capabilities on Earth, provide intelligence and communication functions, and achieve international esteem. Russia is reactive to US strategy and counterspace technologies. The latter, including electronic weapons that can jam satellites, have been developing to provide Russia with an asymmetrical edge to offset US military advantages. Hence, military efforts are but one part of a complex set of tools, employed to navigate what Russia perceives as an increasingly hostile world. Already in 2011, Russia brought about certain institutional modernizations creating the Russian Aerospace Defence Forces which are meant for space security-related activities (► Chap. 21, “Russia’s Space Security Policy”). The Federal Space Program 2016–2025 places emphasis on telecommunication satellites and the need for space technology to generate direct socioeconomic benefits. In March 2018, the Russian Defense Minister Sergey Shoigu stated that Russia must deploy a modern fleet of military satellites to support its army and navy. To quote him: “only with support from space will it be possible for the Armed Forces to reach maximum effectiveness” (DIA 2019). However, Russia’s economic, military, and technological weaknesses compared to the United States and NATO have led Russia to pursue asymmetrical tactics which include working through bilateral bodies and those affiliated through the UN on space policy (► Chap. 21, “Russia’s Space Security Policy”).

Russia can be considered today as having the most complete launch program in the world. Russia currently operates four types of launch vehicles, the Rockot, Soyuz, Zenit, and Proton. The “Russian Space Launch Program” chapter explains how Russia has been successfully engaged in space activities for more than 60 years, having entered the space age as part of the Soviet Union and striding on as a separate state. On the one hand, after the dissolution of the USSR, Russia inherited the large scientific and technical potential and technological developments of one of the two most powerful space nations of that time. But on the other hand, Russia was deprived of a large part of technologies and infrastructure put in place earlier. The launch vehicles that used to be Soviet became foreign, and the key launch site turned out to be located outside Russia’s national territory. Also, it proved to be difficult for Russia to use remnants of its own technologies. For Russia, space is thus not only a question of national defense and security or its position in the market of commercial launch services but also, and more importantly, a question of the status of Russia as a highly

developed nation in terms of science and technology (► Chap. 60, “Russian Space Launch Program”).

### Key Priorities

The priorities and trends in space security as seen in the countries and regions presented above can be grouped in Fig. 2 below. The identified space, security, and defense priorities areas are related to “Security from Space” and “Security in Space.” The “Security from Space” priorities constitute: (1) disaster management, (2) resource management, (3) transport and communications, (4) environment, climate change, and sustainable development, (5) external security including foreign policy and border surveillance, (6) internal security including support to justice and home affairs, (7) military, and (8) financial. The “Security in Space” priorities constitute: (1) defensive space security and control, (2) offensive space security and control, (3) space surveillance and tracking, (4) space weather, (5) near earth objects, (6) orbital debris mitigation, (7) space traffic management, (8) active debris removal, and (9) access to space. These trends demonstrate an evolution of European countries priorities from strictly civil-oriented applications to also encompassing security and defense ones. The grouping of priorities allows for a clear overview of the status of space security. However, the lack of explicit boundaries between “safety,” “security,” and “defense” makes it rather difficult to clearly distinguish among the different positions of countries and regions. In some countries it seems that space security is closer to the safety side (i.e., Africa, UAE), while in others it is closer to the defense side (i.e., the United States, Russia). Several countries in the regions presented have demonstrated a clear shift of their space policy and programs



Fig. 2 Priorities for space security in space and from space across countries/regions

from safety to defense, notably Japan. In some cases, it is even more ambiguous to identify an approach due to the absence of a regional understanding such as in Africa and Latin America.

---

## **Concluding Remarks: The Way Forward for Space Security**

The significance of outer space as a strategic focal area with geopolitical consequences is widely recognized. Outer space, which was perceived during the Cold War as another theatre of operations for the United States and the former Soviet Union, has now become a common strategic medium for governmental and non-governmental activities around the world. Accordingly, the concept of space security has been changing over time. Traditional defense strategic concepts remain relevant in the face of hybrid threats, counterspace, and proposed Space Forces rendering thereby space as a warfare domain. Even though space security used to consist of exclusively military and defense elements in states' relations, it has evolved to encompass increasing activities of private and commercial actors and their implications for safety and sustainability. In this regard, space security cooperation ensuring the peaceful uses of outer space is absolutely necessary.

The wide range of space security perceptions has been further intensified by the technological and organizational transformation of the outer space environment. The increasing technological advances; the growing interdependencies between governmental, civilian, and commercial actors; and the emergence of the civil-military paradigm have created diversified interests across countries and regions in the world. In this context, multifaceted and interactive space security perspectives with ranging safety, security, and defense elements present a rising concern for cooperation mechanisms in place. Hence, the debated and different understanding of the concept of security is reflected in the various policies and programs across the world, emphasizing the civil-military nexus and the associated challenges. Definitions and concepts of what is encompassed by the term "space security" are diverse, imprecise, and evolving along the strategic priorities and needs of countries and regions. This presents problems when endeavoring to build cooperative approaches among diverse actors. The definition provided in this Handbook allows to structure the uncertainty created by the multitude of definitions, while allowing to reach a common understanding fostering cooperative and collective frameworks in space security. This definition allows to approach space security in its full spectrum capturing all elements of space security instead of differentiating among the various conditions. Hence, the definition manages to resolve the civil-military challenge by incorporating it in a flexible manner instead of turning it into a fixed and obsolete concept. In line with the principles of international cooperation and peaceful uses of outer space, this definition ultimately enables common understanding which is a starting point aiming to ensure strategic stability at the international level.

Based on this definition, the way forward for space security calls for its operationalization through the development of stability-enhancing mechanisms that tackle



the challenges of the evolving security notion. Such mechanisms should be underpinned by mutually understood concepts that are translated in a comprehensive regulatory solution at the international level. In this direction, recent developments at the UNISPACE+50 process, prepared by the United Nations Office of Outer Space Affairs in 2018, have considered the development of international legal mechanisms that cope with the broader concept of space security – safety, security, and sustainability. In this regard, Space Traffic Management (STM) is considered as a solution that can ensure space security in the broad sense by resolving practical concerns of the international community, such as in-orbit collisions and interferences. The definition of the STM in the 2006 International Academy of Astronautics Cosmic Study as “the set of technical and regulatory provisions for promoting safe access into outer space, operations in outer space and, return from outer space to Earth free from physical and radio-frequency interference” complements the operational side of the space security definition in this chapter. Hence, STM can serve as the basis of ensuring space security while safeguarding the principles of international cooperation and peaceful uses of outer space.

---

## References

- African Union (2015) An overview of the Agenda 2063, First Ten Year Implementation Plan. Retrieved from [https://au.int/sites/default/files/documents/33126-doc-11\\_an\\_overview\\_of\\_agenda.pdf](https://au.int/sites/default/files/documents/33126-doc-11_an_overview_of_agenda.pdf)
- African Union (2017) African space strategy – Towards Social, Political and Economic Integration, Second Ordinary Session for the Specialized Technical Committee Meeting on Education, Science And Technology (Stc-Est) 21 October To 23 October 2017, Cairo, Egypt. Retrieved from [https://au.int/sites/default/files/newsevents/workingdocuments/33178-wd-african\\_space\\_strategy\\_-\\_st20445\\_e\\_original.pdf](https://au.int/sites/default/files/newsevents/workingdocuments/33178-wd-african_space_strategy_-_st20445_e_original.pdf)
- African Union (2020) First continental report on the implementation of Agenda 2063, African Union Development Agency, 8 February 2020. Retrieved from [https://au.int/sites/default/files/documents/38060-doc-agenda\\_2063\\_implementation\\_report\\_en\\_web\\_version.pdf](https://au.int/sites/default/files/documents/38060-doc-agenda_2063_implementation_report_en_web_version.pdf)
- Baldwin DA (1997) The concept of security. *Rev Int Stud* 23:5–26
- DIA (2019) Challenges to space security. Defense Intelligence Agency, Washington, DC
- Euroconsult (2019) Government space programs – benchmarks, profiles, and forecasts to 2028. Euroconsult, Paris
- Giannopapa C (2011) Improving Africa’s benefit from space applications: the Europeane-African partnership. *Space Policy* 27:99–106. Elsevier
- Giannopapa C, Adriaansen M, Antoni N, Schrogl K-U (2018) ESA’s policy on space and security. *Acta Astronautica* 147:346–349
- Government of Canada (2019) Exploration imagination innovation – a new space strategy for Canada, Ministry of Innovation, Science and Economic Development. Retrieved from <https://www.asc-csa.gc.ca/pdf/eng/publications/space-strategy-for-canada.pdf>
- Greenwood C (2011) Self-Defence. In: Max Planck Encyclopedia of Public International Law. Oxford University Press, Oxford, April 2011
- Harding RC (2015) Emerging space powers of Latin America: Argentina and Brazil. In: Al-Ekabi C, Baranes B, Hulsroj P, Lahcen A (eds) *Yearbook on space policy 2012/2013*. Springer, Vienna
- Hitchens T (2019) Space traffic management: U.S. military considerations for the future. *J Space Saf Eng* 6:108–112

- Jiang H (2019) Programme and development of the “Belt and Road” Space Information Corridor, CNSA at 2019 United Nations/China Forum on Space Solutions. Retrieved from [https://www.unoosa.org/documents/pdf/psa/activities/2019/UNChinaSymSDGs/Presentations/Programme\\_and\\_Development\\_of\\_the\\_Belt\\_and\\_Road\\_Space\\_Information\\_Corridor\\_V5.1.pdf](https://www.unoosa.org/documents/pdf/psa/activities/2019/UNChinaSymSDGs/Presentations/Programme_and_Development_of_the_Belt_and_Road_Space_Information_Corridor_V5.1.pdf)
- Komiya Y (2016) Basic plan on space policy, implementation schedule (Revised FY2015). Retrieved from Japan Space Forum 2016: [http://www.jsforum.or.jp/stableuse/2016/pdf/6.%20DG\\_Komiya.pdf](http://www.jsforum.or.jp/stableuse/2016/pdf/6.%20DG_Komiya.pdf)
- Lal B, Balakrishnan A, Caldwell BM, Buenconsejo RS, Carioscia SA (2018) Global trends in space situational awareness (SSA) and space traffic management (STM). IDA Science and Technology Policy Institute, Washington, DC
- McDonald A, Brollowski H (2011) Security. In: Max Planck encyclopedia of public international law. Oxford University Press, Oxford
- National Defense (2020) Middle East Allies look to expand space capabilities. Retrieved from <https://www.nationaldefensemagazine.org/articles/2020/2/3/middle-east-allies-look-to-expand-space-capabilities>
- Nie M (2020) Space privatization in China’s national strategy of military-civilian integration: an appraisal of critical legal challenges. Space Policy. In press, 2020,101372, ISSN 0265-9646
- Osisanya S (2015) National security versus global security. United Nations Chronicle. Retrieved from <https://www.un.org/en/chronicle/article/national-security-versus-global-security>
- Republic of South Africa (2018) National Space Science and Technology Programme Strategy, To leverage the benefits of space science and technology for socio-economic growth and sustainable development. Retrieved from <https://www.sansa.org.za/wp-content/uploads/2018/05/National-Space-Strategy.pdf>
- Robinson J (2018) Cross-domain responses to space hybrid provocations via economic and financial statecraft. The Prague Security Studies Institute, Prague, Czech Republic
- Rothschild E (1995) What is security? The MIT Press on behalf of American Academy of Arts & Sciences, MIT Press 124:53–98
- Sarli BV, Cabero Zabalaga M, Telgie A (2018) Review of space activities in South America. J Aeronaut Hist 8:208–232
- Sheehan M (2015) Defining space security. In: Schrogl K-U et al (eds) Handbook of space security: policies, applications and programs. Springer, New York
- SpaceNews (2020) Space force-sponsored study to assess capabilities of commercial industry. Retrieved from <https://spacenews.com/space-force-sponsored-study-to-assess-capabilities-of-commercial-space-industry/>
- Spacewatch.global (2016) Iranian satellites to share information system of the Asia Pacific Space Cooperation Organisation. Retrieved from Spacewatch.global: <https://spacewatch.global/2016/09/iranian-satellites-share-information-system-asia-pacific-space-cooperation-organisation/>
- Spacewatch.global (2019) Military space: Japan and United States pledge mutual defence cooperation in space, cyber. Retrieved from <https://spacewatch.global/2019/04/military-space-japan-and-united-states-pledge-mutual-defence-cooperation-in-space-cyber/>
- Tarikhi P (2015) The Iranian Space Endeavor. Springer International Publishing, Cham
- U.S.FR (2018) Space policy directive-3, National Space Traffic Management Policy, US Federal Register, 18 June 2018, 83 FR 28969, 2018-13521. Retrieved from <https://www.federalregister.gov/documents/2018/06/21/2018-13521/national-space-traffic-management-policy>
- United Nations (1967) Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and other Celestial Bodies, Article I, 27 January 1967, 18 UST 2410; 610 UNTS 205; 6 ILM 386 (1967)
- United Nations (2019) General Assembly, First Committee, First committee delegates exchange divergent views on how best to prevent weaponizing outer space, cyberspace amid eroding global trust, GA/DIS 3636, Seventy-fourth session, 17th & 18th meetings, 29 October 2019. Retrieved from <https://www.un.org/press/en/2019/gadis3636.doc.htm>

- UNOOSA (2019) The African space policy and strategy, towards social, political and economic integration of Africa, Dr. SALEY Mahaman Bachir, African Union Commission, United Nations China Forum on Space solutions, 24–27 April 2019 - Changsha – China. United Nations Office for Outer Space Affairs
- UNSPIDER (2010) VI Space conference of the Americas. United Nations Platform for Space-based Information for Disaster Management and Emergency Response (UN-SPIDER), November 2010. Retrieved from <http://www.un-spider.org/news-and-events/events/vi-space-conference-americas>
- Williams PD (2013) Security Studies: An Introduction. Routledge, Oxford University Press



# Challenges to International Space Governance

# 3

Ahmad Khan and Sufian Ullah

## Contents

Background .....	36
Challenges to International Space Governance .....	37
Increasing Competition in Space .....	37
No Consensus on Space Arms Control .....	38
Increasing Reliance on Space Assets .....	38
Security-Driven Self-Interests of States .....	39
Dual-use of Space Assets .....	39
The USA, Russia, and China in Space .....	41
Proliferation of ASAT Weapons .....	42
Stalemate on Arms Control Treaty Negotiations .....	43
Conclusion .....	46
References .....	47

## Abstract

Space is now a congested, contested, and competitive domain. Space technologies and programs have become vital ingredients of major spacefaring nations' national power. In the past three decades, space has gained importance for security and socioeconomic development of spacefaring nations. However, most of the activities in this domain are unchecked primarily due to lack of an internationally agreed treaty in space. In addition, the challenges to international space governance in ensuring space as a safer and more secure environment are

---

A. Khan (✉)

Department of Strategic Studies, National Defence University, Islamabad, Pakistan  
e-mail: [ahmad\\_ishsq669@yahoo.com](mailto:ahmad_ishsq669@yahoo.com)

S. Ullah

Department of Defence and Strategic Studies, Quaid-i-Azam University, Islamabad, Pakistan  
e-mail: [sufianullah@gmail.com](mailto:sufianullah@gmail.com)

enormous. These include the increasing pool of actors, growing commercialization, expanding military space programs, the proliferation of anti-satellite weapons, and lack of consensus among states on a conclusive and universally negotiated treaty to prohibit an arms race in space. The expanding number of spacefaring actors and dual-use technologies have made the skies and space more competitive. On top of that, the competing states are following a path from space militarization to weaponization which has aggravated the threat of space war.

---

## Background

Space is a strategic domain in which both major and emerging space powers seek a place. States are shifting gears to maintain their position in space in twenty-first century primarily because of both military and economic benefits. After the end of Cold War, the world is witnessing a gradual increase in the military and peaceful space assets and technologies of states other than USA and Russia. States like India, China, Japan, South Korea, etc. are expanding their international partnership to send other states' satellites in outer space. This has made space a competitive domain; in fact, China and India have sent provided alternative platforms for developing countries to send their satellites more cheaply than from the USA and Russian launching pads. Key challenges to making space a more safe and secure environment include the increasing pool of actors, growing commercialization, expanding military space programs, and lack of agreement by states on a conclusive and universally negotiated treaty to prohibit an arms race in space. The expanding number of spacefaring actors has made the skies and space more competitive. Likewise, these factors are increasingly contributing toward key challenges to international space governance and ensuring space remains a safe and secure domain for commercialization and scientific exploration.

To pursue scientific endeavors and to meet commercial as well as security needs, the reliance of states on space-based capabilities has increased significantly. Along with the commercial and economic uses of space, states have been ambitiously investing in military exploitation of this *global commons* that has now emerged as an arena of potential confrontation. While space has a lot to offer to human growth and prosperity, this potential is hijacked by risks of conflict escalation. The recent trends in technological developments suggest that the space is being rapidly weaponized with little prospect of establishing an agreeable and verifiable framework for global space governance. Divergent policy approaches, coupled with competing strategic aspirations, constrain pursuit of collective action toward achieving this goal. Space activities are generally categorized into three sectors including civilian, military, and commercial. This chapter focuses on the military sector to explicate what drives the arms competition in outer space and argues that cooperation and space governance may enhance mutual security and decrease possibilities of conflict. However, the primary challenge to this is that states tend to see the domain of space as a field of competition whereby one's considerable presence equates to enhanced national

stature among the comity of nations. One such example is recently witnessed euphoria among Indian leaders after the country successfully test fired its first Anti-Satellite (ASAT) weapon system.

---

## Challenges to International Space Governance

Currently, spacefaring nations seek to establish decisive dominance at least in the military aspect. This approach consequently heightens competition by stimulating tensions and encouraging military countermeasures. Given the ongoing geopolitical competition in space, whereby this domain has emerged as the fourth medium of warfare, any model for space governance must not overlook the inherent competitive tendencies among states, and should rather aim to promise more incentives through cooperation (Khan and Khan 2019). The rationale behind global space governance revolves around the notion that despite having competing interests, the irrational behavior of spacefaring nations would be equally disadvantageous for their pursuits in this domain. Recognizing the states' inherent instinct to pursue competitive objectives, this chapter suggests cooperation toward space governance in a manner that does not overlook their grounded self-interest but aims to reduce threats in a cooperative manner. The idea of global space governance, therefore, seeks to maximize the prospects of peaceful exploitation of this *global commons* by encouraging responsible behavior.

## Increasing Competition in Space

Spacefaring nations are developing their space programs at a fast pace. What really drives this unabated exploitation of space is a question that largely remains unaddressed. While some argue that these programs are driven by “techno-nationalism” to demonstrate technological prowess, a state's natural instinct to hedge against the others in a *global commons* also cannot be ignored (Sheehan 2010). Likewise, since an advanced space program is an indication of nation's military and industrial strength, states tend to see progress in this domain as a token of national prestige (Mission Shakti . . . 2019) (One such example is Prime Minister Narendra Modi's statement after India conducted a successful Anti-Satellite Missile Test on 27 March 2019. Notwithstanding that the experts raised concerns regarding possible negative implications that ASAT's debris may have, Prime Minister Modi asserted that this capability placed India among the handful of space superpowers).

While the USA and Soviet Union were the only competitors for supremacy in space during the Cold War, the post-Cold War era has witnessed new entrants in this competition – all aiming to secure advantageous position through dual-use capabilities. The ongoing trends of commingling space and counterspace capabilities give rise to new warfare strategies that not only implicate national securities of other states but also undermine the prospects of peaceful exploration of outer space.

## No Consensus on Space Arms Control

One reason behind states' reluctance to enter into any space-related arms control agreements can be the urge to amass maximum technological capabilities. It appears that the major actors intend to buy maximum possible time to develop enough capabilities before fully agreeing to put limits to numbers and types of their capabilities. Nevertheless, it must be realized that the future of global arms control considerably depends upon the arms buildup in the domain of space. If an arms race in space continues to go unchecked, it would seriously jeopardize other efforts to arrest arms competition. The primary reason behind this is the growing diversity of space-based military assets and their unfolding roles in different military strategies. One such example is nuclear deterrence.

## Increasing Reliance on Space Assets

Ever since the launch of first satellite in outer space, reliance on space has only increased. The rapid scientific and technological advancements have surged the utilization of outer space for wide range of purposes. Also, the exploitation of this *global commons* no longer remains the prerogative of a handful of great powers; rather even the developing countries are now the beneficiaries of this domain. The enhanced reliance on space-based assets for a wide range of operations – like remote sensing, communication, and so on – further necessitates effective global space governance that could ensure the favorable environment for peaceful ventures. While our dependence on space has immensely increased in the past few decades, the international community has failed to adequately respond to the rising threats and vulnerabilities. A state's reliance on space assets is directly proportional to the increasing risks, vulnerabilities, and challenges to its operational space assets. The more the numbers of space assets are operationalized, the more vulnerable they are to attacks in space from the state adversary that also includes non-state actors. The superpowers in Cold War era took a promising start in the form of new treaties and norms to develop consensus in achieving a peaceful outer-space environment. In the 1960s, both the rivals carried out nuclear explosions above the atmosphere but later agreed on non-testing of nuclear weapons in atmosphere and have complied with this restriction so far. However, with passing times, the international community has largely failed to develop a concrete mechanism to avoid evolving threats confronting a peaceful environment in space.

The competitive or cooperative engagement among states dates back to the Cold War period when the two superpowers were engaged in the Moon race and sought to develop space-based capabilities to support their military and intelligence operations. The space endeavors of the two adversaries seemed to be driven more by the struggle for political and military advantages, instead of pursuit of scientific explorations. Although the two states agreed on peaceful cooperation in space after the Apollo-Soyuz Test Project emerged as a symbol of détente between the competing superpowers in the 1970s, their continued fight for preponderance in this domain converted space into a battleground of the arms race ([Apollo-Soyuz Test Project](#)).

## Security-Driven Self-Interests of States

The key challenge to global space governance remains in the very nature of states' behavior. As argued earlier, the self-interested members of international community generally tend to overlook the negative consequences of their behavior and only seek to maximize their benefits. Particularly in the absence of shared strategic goals, states find it difficult to compromise their ambitions and accept limitations on the behavior that otherwise promises relative advantages. In this context, what may encourage states to enter into arms control arrangements is the realization of their mutual vulnerabilities in a destabilizing environment. Likewise, putting "high value on collective benefits" may also encourage them to avoid any irresponsible behavior that could threaten the international peace and security. Therefore, as rightly identified by Thomas Schelling and Morton Halperin, the threefold objectives of any arms control arrangement include reducing the likelihood of occurrence of war, costs of preparations, and destructive consequences of war (Larsen 2002).

At present, states joining hands to develop and operate the International Space Station, joint production and launch of satellites, and greater integration in the use of space-based services such as communication networks are testament of ongoing international cooperation in this domain. While it hints at the huge prospects of any mutually agreeable governance framework, the same is also marred by significant challenges owing to differing aspirations of states toward this domain. Besides peaceful uses of these capabilities, the security implications of space-based technologies are driving interstate competition. Along with jointly pursued peaceful uses, great powers have been exploiting space for their vested military advantages, thus depicting the emerging face of interstate relations where strategic rivalries predominantly define the geopolitical environment. The diverse use of space applications, where the distinguishing line between peaceful and military use of space-based capabilities is too blurry to clearly reflect the difference, further exacerbates one's urge to misinterpret other's actions and respond accordingly. One such example is Global Positioning System (GPS) that, despite it enabling a huge array of peaceful uses in different activities, is considered as a military capability (Ohlandt 2014). Likewise, even the high-resolution commercial remote sensing satellites, which can strengthen stability by providing a real-time picture of an adversary's military operations, may also be used for missile warning, target identification, and other military roles.

## Dual-use of Space Assets

The political consequences of the employment of dual-usable assets in space are undesirable. If one were to see the role of military capabilities in geopolitical competition among great powers, it would be plausible to assume that the military values that competing powers attach to their space capabilities would be of paramount significance in shaping the evolving great power competition.

Since the international anarchic system offers no guarantee that a state with considerable military power would not use it in an offensive manner to subdue



others, it is only natural that the rival states view each other's technological advancements with skepticism and may even resolve to respond in kind. This is particularly significant in an environment that lacks institutional structures that could assure general security by regularizing the behavior of states and ensuring transparency. It consequently generates a security dilemma that continues to fuel the mutual mistrust, intensify the prevailing arms race, and diminish the prospects for global space governance (Jervis 1978). (Robert Jervis defined security dilemma as a state of affair in which security of one state decreases the security of another state.) Since one state's accumulation of power, as put by John Herz, makes others feel insecure and compel them to take remedial measures, this consequently leads to chain reaction that undermines general security (Herz 1950).

The inherent "ambiguous symbolism" of technology, as referred to by Ken Booth and Nicholas J. Wheeler, makes the security dilemma more intense as other states may see one's weapons as offensive or defensive depending on their own presupposition and threat perceptions (Booth and Wheeler 2008). The ambiguity regarding a dual-use capability is particularly more intense in the domain of space. The claimed roles of space-based assets may alter dramatically during peace and the times of crises. The dilemma of interpretation and dilemma of response are therefore the two most significant factors that constrain the pursuit of agreeable governance structures in the domain of space (Booth and Wheeler 2008).

When a state develops a certain military capability, the leadership of a rival state confronts the dilemma of interpretation in ascertaining whether that development is for offensive purpose or it is just a measure to bolster defensive capability. Likewise, the dilemma of response also constrains one's options to respond to any such development by adjusting force posture. The traditional response of a state in an uncertain environment may include disengagement from other actors and arms development and deployment. If the state goes for such an action that generates military confrontation, it leads to mutual hostility and further diminishes the prospects of reducing threats through cooperation. In such an environment of uncertainties, the best course of action that a state can think for itself, as put by John J. Mearsheimer, is to maximize its relative power and be a hegemon in the system by ensuring that there is no peer competitor with equally offensive or overwhelming capabilities (Mearsheimer 2013). After land, air, and sea, space has now emerged as a domain where competing powers vehemently pursue predominance through technological advancements and refrain, at least at the moment, from committing to limitations on this pursuit.

Such an understanding of security dilemma in international politics is evident from Chinese and Russian perceptions of growing US presence in space. The USA has long maintained unequivocal supremacy in space by virtue of its unmatched civilian as well as military space capabilities. While it successfully superseded Soviet Union in this rivalry for hegemony, China has recently emerged as the most potent competitor to US dominance in this domain. As put by Defense Intelligence Agency, adversary's integration of space and counterspace capabilities into military operations pose a challenge to US space dominance (Challenges to Security in Space 2019). The notion of "congested, contested, and competitive" space domain

also signifies how the USA views the growing adversarial capabilities that may erode its strategic advantage. Thus, the USA considers it imperative to deny space to its rivals (Outer Space Increasingly 2012).

## The USA, Russia, and China in Space

The USA, Russia, and China are currently the major space powers – with India trying to steadily catch up – which have developed significant space-related weapon systems. These states possess the most sophisticated capabilities and have also shown the intent to test and launch space-based weapon systems.

Russia sees the US space-based capabilities in connection with the growing asymmetries in the military equilibrium between the two states and seeks to contain the USA by modernizing its own assets (Zervos 2011). The USA believes that China and Russia seek to challenge the US position in space, exploit its dependence on space-based assets, and reduce its military effectiveness through counterspace capabilities (Challenges to Security in Space 2019). Given that there are no serious efforts to address disagreements over a desirable code of conduct in space, the strategic distrust among them continues to grow. For China, the advanced space program is a means to project its soft power in terms of technological development and also to accrue strategic advantage by challenging the US supremacy.

With China surpassing Russia as the second leading space power, the US-China rivalry in space may have grave implications for global peace and security. China has been emerging as a rising global power, and its increasing footprint in space now challenges decades-long US supremacy. The two strategic rivals are skeptical of each other's technological developments and space capabilities. This situation is further exacerbated in the absence of any concrete dialogue mechanism over a prospective agreeable code of conduct in space. There have been perceptions within China that the US-led space weaponization not only implicates peaceful uses of outer space but also is also driven by an intent to neutralize China's nuclear deterrent capability (Zhang 2008). This growing fear has shaped the Chinese behavior on two different accounts: at strategic level, it resolves to take the countermeasures and enhance its own space capabilities to neutralize any such threats, and at diplomatic level, it strongly advocates the Prevention of Placement of Weapons in Outer Space Treaty (PPWT) to prevent weaponization of outer space. CD first proposed PPWT in CD in 2008. In addition to these concerns, projecting its own space power has also become paramount for China to register itself as a rising power that could position itself among the other advanced spacefaring nations (Khan and Khan 2019). While dominating space, these developments also exacerbate US fears of a "Space Pearl Harbor," thus contributing to unending security spiral where action-reaction dynamics result in unending arms race (Commission to Assess United States National Security Space Management 2001). (The term "Pearl Harbor" has gained the salience of a metaphor for being caught unaware. The 2001 Space Commission of the USA cautioned of a Space Pearl Harbor stating that the USA needed to be better

prepared as its assets in space were vulnerable against a surprise attack.) This is particularly evident in the development of a more destabilizing capability, i.e., the anti-satellite weapons system. China tested its ASAT missile capability in 2007 when it launched SC-19 interceptor to hit a defunct satellite at an altitude of 865 kilometers. A year later, the USA also demonstrated its capability to neutralize a failed satellite with an SM-3 missile. Though an ASAT capability is a Cold War technological development, this development suggests that states are moving on a path from space militarization to weaponization.

The USA emphasizes on sustaining its supremacy in space while ensuring its “freedom of action,” by dissuading or deterring others from developing similar capabilities (National Space Traffic Management Policy 2018). Such hegemonic aspirations, combined with Chinese and Russian resolve to challenge US predominance, set the stage for potential conflict.

### **Proliferation of ASAT Weapons**

Besides its claimed deterrent imperatives, India’s testing of ASAT weapon system appears to signify a symbol of national pride and prestige. However, the destabilizing consequences of this technology far outweigh such potential benefits, thus posing a question on the strategic and military rationale behind its development and operational deployment. Introduction of ASAT weapon systems only exacerbates the risks of crisis escalation and eruption of conflict at lower levels. By reducing the early warning capability or disrupting the satellite-dependent communication channels, the ASAT weapon directly undermines one state’s ability to effectively retaliate against a possible strike that implicates the strategic stability (Oznobishchec 1989). Likewise, ASATs are also inherently aggressive weapon systems that increase the vulnerabilities of other state’s command and control & intelligence, information, surveillance, and reconnaissance (I<sup>2</sup>SR) systems against a possible attack. This particular attribute of neutralizing some of an adversary’s critical infrastructures makes ASATs a potent counterforce weapon. It consequently not only raises nuclear alert levels but also emboldens response options that may not remain within the confines of the law of proportionality (Ullah and Imam 2019). This scenario only contributes to an uncertain strategic environment and intensifies the dilemmas of interpretation and response by increasing the element of unpredictability between the two adversaries (Lele 2019). In a nuclear environment, the possessors of this capability may argue for the deterrent role of ASAT weapon systems and consider this capability as a contributor to strategic stability (U.S. Anti-Satellite (ASAT) Program 1987). (For instance, the USA has since long considered its ASAT program as an essential component of its deterrence.) However, the aforementioned aspects suggest that ASAT weapon systems may only have some role in fighting a war, but not in averting one, and thus contribute very little deterrent value. ASAT weapons can put at the risk the very satellites – including early warning systems, communication satellites, and so on – which are believed to be vital for strategic stability.

There is also a possibility that given the growing vulnerabilities to space-based assets, particularly in context of kinetic or other threats to revolving satellites, states may eventually resolve to invest more in ground-based and aerial systems to ensure survivability of their critical infrastructures. Major powers need to realize that any use of ASAT weapons in counterforce roles may lead to crisis instability and possible nuclear escalation. Besides these growing risks of escalation, the kinetic use of weapons in space, as argued by Michael Krepon, would be self-defeating (Krepon 2013). For instance, the use of ASAT offers limited military advantage as the resulting debris would pose an equally dangerous threats to one's own space assets. By recognizing this inherent character of ASAT weapon, major stakeholders may attempt to develop consensus on considering this tool of warfare as a destabilizing weapon. This would not only reinforce strategic equilibrium in space but also pave way toward more encompassing arms control mechanisms.

### **Stalemate on Arms Control Treaty Negotiations**

Given that the military and peaceful uses of space-based technologies generate competition among spacefaring nations, the undesirable political and strategic consequences of this arms race require that concerted efforts be made to reach a legal framework to govern space. As the advancing technologies offer more potent and survivable space weapon systems and the distinguishing lines between civilian and military use of space capabilities become more blurred, the chances of accidental use of weapons would increase the dangers of crisis instability. The continued dismissive attitude of concerned states would steadily bring us closer to a point where it will be difficult to arrest the buildup of space-related weapons systems. Further delays in reaching an agreeable legal framework of governance will result in increasingly irresponsible behavior involving ambitious use of military capabilities in this global common.

Unlike other domains of warfare including air and sea, space is more prone to risks of collateral damage as any disruption of infrastructure would also directly implicate international commercial ventures. The debris caused by any kinetic-energy warfare would not only implicate military satellites of competing states but also result in unstable space environment for all stakeholders. It is, therefore, important that all spacefaring nations push for collective action to reach an agreeable mechanism to put limits on weaponization of space and work toward creating a more transparent environment in space. Nevertheless, collective action is a function of mutual trust and transparency. The lesser the security dilemma, the greater are the prospects of developing consensus. It is the uncertain environment in space that has thus far prevented states from achieving that level of mutual trust. The Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, commonly known as the Outer Space Treaty (OST) serves as a baseline for a collective action. It recognizes space as a potential "province of all mankind" and emphasizes the

peaceful exploration of this *global commons* (Treaty on Principles Governing the Activities of States 1967). The major provisions of the Treaty call for adherence to international law to ensure international peace and security, agreement on not to place nuclear weapons in Earth orbit or on any celestial body, and establish liability for damages. (Article III of the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, deals with the provision related to adherence to international law. Article IV provides for a commitment on not to place weapons of mass destruction in outer space. Articles VI and VII deal with the liability clauses and specify that the state parties to the Treaty shall be responsible for their national activities. Any activities in space carried out by nongovernmental entities would require authorization by the concerned national authority, and the latter shall be held responsible for any violations to the principles of the Treaty.) Though the Treaty offers a foundation for further global cooperation through more treaties, a number of shortcomings in the scope of the Treaty serve as obstacles in achieving this broader goal. These include, first, the anarchic nature of international system whereby there is no central authority to regulate the behavior of states. Second, there is no effective verification mechanism to check the member states' compliance with agreed framework, and the OST regime has largely failed to generate collective action toward ensuring well specified and rules-based global space governance. Third, as pointed out by Nancy Gallagher and John D. Steinbruner, the states are unwilling to offer transparency about their technical ventures and tend to classify these developments under secrecy (Gallagher and Steinbruner 2008). It only exacerbates the dilemma of interpretation for adversarial states in assessing the true motivations of other states. Fourth, to arrest the weaponization of space, the Treaty only banned placement of weapons of mass destruction in space. The limited scope of the Treaty thus could not address the post-Cold War evolving trends in the development of space weapons including the Conventional Prompt Global Strike capabilities, ASAT weapons, and their technological links with the antiballistic missile systems.

Effective space governance requires that in absence of a central authority that could verify compliance, spacefaring nations take on the responsibility and observe restraint though voluntary or less formal means. Eligar Sadeh suggests that these may include establishing global norms, codes of conduct, confidence building measures, and diplomacy (Sadeh 2015). Nevertheless, the greatest constraint in driving a collective action in this regard remains to be the prevailing mistrust among states and absence of any verification mechanism. Strategic distrust among major spacefaring nations demonstrates how growing mistrust may put existing legally binding commitment in jeopardy. This challenge is further magnified in an environment where there are no verification mechanisms to ensure member states' compliance to the agreed framework.

The divergent approaches of major spacefaring nations toward global space governance further add complexities to the problem. While the USA and its allies, including the European Union (EU) and Japan, argue for an international code of

conduct that could enhance rules-based space order, China and Russia emphasize negotiating a treaty to prevent an arms race in outer space (Krepon 2013). The divergent approaches of different states are partially shaped by how they viewed the defunct Anti-Ballistic Missile (ABM) Treaty between the USA and Russia. Many legal experts held the opinion that this bilateral treaty directly dealt with the weaponization of space as it included the space-based ABM systems (Johnson-Freese 2007). For three decades, ABM Treaty proved to be an effective tool to prevent deployment of space weapons, but US withdrawal from the Treaty in June 2003 was a serious blow to the norms against weaponization of space. Withdrawal from this Treaty created incentives for the USA to deploy space-based element of its multilayered missile defense system and also other war-fighting capabilities as part of military uses of space (Outer Space and Global Security 2003). The vacuum created by US decision to withdraw encouraged states not parties to the treaty to press for a treaty-based mechanism to ban use of weapons in outer space. Furthermore, in February 2008, Russia and China jointly drafted and submitted a Prevention of the Placement of Weapons in Outer Space (PPWT) Treaty in Conference on Disarmament to prohibit the weaponization of space. However, the USA opposes the proposed PPWT as it continues to vote against the UN Resolutions prohibiting an arms race in outer space.

The key difference among states remains what constitutes a weapon in space. Also, states tend to justify their space programs while highlighting the deterrent value of their infrastructure. However, even if a weapon is placed in space for defensive purposes, its ambitious and aggressive use would have irreversible consequences for strategic stability as well as peaceful exploration of space. This necessitates that efforts be made to develop consensus on destabilizing implications of certain types of technologies and outlaw the development and placement of those weapon systems in outer space. After having successfully developed a consensus on placement of nuclear weapons in space, global peace and stability requires that similar restrictions be placed on the testing and placement of ASAT weapon systems. By pursuing arms control to constrain the growth of ASATs, the dangers of escalation and preemptive first strikes may be averted. The first requirement for a peaceful or rules-based governance structure for space is to ensure the survival of satellites. The proposals that emphasize only regulating behavior in space tend to overlook the anarchic nature of the system and states' urge to maximize their relative gains, which often lead to an irresponsible behavior without any regard for the negative consequences for other states (Defrieze 2014) (For instance, it is emphasized that regulating and punishing behavior is the best approach to control the weaponization of space).

Through cooperative engagements, transparency may be ensured to minimize the security dilemma. At present, it appears that the ongoing technological developments and innovations in space programs also cause the dismissive attitude toward arms control. Major powers are seemingly buying time to accumulate maximum capabilities as they are also not sure about the status of research and development in adversary's space programs. This raises the level of uncertainty.

## Conclusion

We conclude that states are following a path from space militarization to weaponization. This indicates that states have the capability to weaponize outer space depending on the political, economic, and strategic circumstances at the global and regional levels. The growing number of actors in outer space has increased space traffic, makes space assets more vulnerable, and creates incentives for major spacefarers to take offensive countermeasures to protect their space assets. Their reliance on space assets has been increased as well as the future requirements to conduct combat missions on the ground. Therefore, outer space has become a strategic field for the major powers. There is a possibility of deployment of weapons in the outer space, which could create conflicts of interest among the nations. Therefore, space is now a strategic domain that could play a determining factor in the future engagements. The US unilateral withdrawal from the ABM Treaty in June 2002 and its initiation of Ballistic Missile Defence (BMD) have prompted Russia and China to revisit their strategic force posture. Both countries are continuously increasing their military capabilities at a moderate level, because of the US missile defense system in Europe and in the Far East. Because of this, there is a chance of horizontal proliferation of space weapons in the world. Now, there is a possibility that emerging space powers in view of their security objectives will move toward building ASATs in upcoming years, which will raise the chances of the vertical proliferation of space weapons.

In the absence of multilateral international agreements to prohibit the weaponization of outer space, there is an urgent need for an international agreement or treaty, which could bar the proliferation of space weapons both horizontally and vertically. In this regard, there is a need to re-evaluate and strengthen prevention of an arms race in outer space (PAROS) issue in CD. The world is facing a looming threat of space warfare. And this threat has emerged as reality due to non-agreement of major powers on framing any legal instrument/treaty which prohibits the weaponization of outer space. Russia and China have proposed several drafts to prevent the weaponization of space, like PPWT and No First Placement of Weapons in Space, but the USA and its allies are not agreeing on such draft proposals. These efforts suggest that Russia and China are not willing to fight the war in space and more inclined toward framing legal instruments to avoid space war. On the other hand, it is the USA which is not interested in having any treaty which restricts its freedom of action in space. The chapter concludes that there is a real threat in space that could germinate the seed of armed conflict. The USA and China don't trust each other, and there is strategic distrust between two adversaries, which could be the triggering point of an armed conflict in outer space. The USA's concerns are emanating from China military and economic rise, and the USA wants to contain China in its region of influence. China considers space to be a building block of its national power. This fosters strategic distrust between two space powers, diminishing chances of cooperation between two states. This also provides incentives for both states to build their military space programs to counter each other's space power. Both countries have developed kinetic and non-kinetic means to disrupt, degrade, and damage each other's space assets. All these efforts are a perfect recipe for

a competition in outer space. Space is one of the *global commons* providing crucial resources for humanity. The competition is relatively new and different from what the world has observed in nuclear and conventional military buildups. The military buildup in outer space has brought a paradigm shift in international security as the fear of war in space would cause catastrophe on the Earth. The problem of space debris in the aftermath of a future space war may last for centuries. Therefore, the development of space weapons on the Earth by major spacefarers and the doctrines and strategy to fight a war in space has brought a paradigm shift in international security.

---

## References

- Apollo-Soyuz Test Project. National Aeronautics and Space Administration. <https://history.nasa.gov/astp/index.html>. Accessed 28 Mar 2019
- Barnes E, William J (2019) Russia has restarted low-yield nuclear tests, U.S. believes. *New York Times*, 29 May. <https://www.nytimes.com/2019/05/29/us/politics/russia-nuclear-tests.html>. Accessed 30 July 2019
- Booth K, Wheeler J (2008) *The security dilemma: fear, cooperation and trust in world politics*. Palgrave Macmillan, Basingstoke, p 43
- Buchan A (1965) The dilemma of India's security. *Survival* 7(5):204–207
- Challenges to Security in Space (2019) U.S. Defence Intelligence Agency, Washington, DC, pp 7, 33
- Defrieze C (2014) Defining and regulating the weaponization of space. *Joint Force Q* 74:110–115. [https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-74/jfq-74\\_110-115\\_DeFrieze.pdf](https://ndupress.ndu.edu/Portals/68/Documents/jfq/jfq-74/jfq-74_110-115_DeFrieze.pdf). Accessed 10 July 2019
- Gallagher N, Steinbruner D (2008) *Reconsidering the rules for space security*. American Academy of Arts and Sciences, Cambridge, p 33
- Herz H (1950) Idealist internationalism and the security dilemma. *World Polit* 2(2):157
- International Space Station. National Aeronautics and Space Administration. [https://www.nasa.gov/mission\\_pages/station/cooperation/index.html](https://www.nasa.gov/mission_pages/station/cooperation/index.html). Accessed 28 Mar 2019
- Jervis R (1978) Cooperation under the security dilemma. *World Polit* 30(2):169
- Johnson-Freese J (2007) Space as a strategic asset. Columbia University Press, New York, p 107
- Khan Z, Khan A (2019) Space security trilemma in South Asia. *Astropolitics* 17(1):4
- Krepon M (2013) Space and nuclear deterrence. In: Krepon M, Thompson J (eds) *Anti-satellite weapons, deterrence and Sino-American space relations*. Stimson Center, Washington, DC, p 33
- Larsen JA (2002) An introduction to arms control. In: Larsen JA (ed) *Arms control: cooperative security in changing environment*. Lynne Rienner Publishers, Boulder, p 2
- Lele A (2019) The implications of India's ASAT test. *The Space Review*, 1 April. <http://www.thespacereview.com/article/3686/1>. Accessed 15 Apr 2019
- Mearsheimer J (2013) Structural realism. In: Dunne T, Kurki M, Smith S (eds) *International relations theories: discipline and diversity*, 3rd edn. Oxford University Press, Oxford
- Mission Shakti Successful, Announces PM Modi. Know All About It (2019) NDTV, 27 March. <https://www.ndtv.com/india-news/mission-shakti-successful-announces-pm-narendra-modi-know-all-about-anti-satellite-missile-test-2013581>. Accessed 31 Apr 2019
- Mowthorpe M (2004) *The militarization and weaponization of space*. Lexington Books, Lanham, p 110
- Ohlandt R (2014) Competition and collaboration in space between the U.S., China, and Australia: Woomera to WGS and the impact of changing U.S. national space security policy. *Asian Surv* 54(2):399



- Outer Space and Global Security (2003) United Nations Publications, Geneva, p vii
- Outer Space Increasingly ‘Congested, Contested and Competitive’, First Committee Told, As Speakers Urge Legally Binding Document to Prevent Its Militarization (2012) Press release no. GA/DIS/3464, October 23. <https://www.un.org/press/en/2013/gadis3487.doc.htm>. Accessed 20 Apr 2019
- Oznobishchec S (1989) Vulnerability of satellites and ASAT weapons. In: Hassard J et al (eds) Ways out of the arms race: from the nuclear threat to mutual security – proceedings of the second international scientists’ congress. World Scientific, London, p 143
- Report of the Commission to Assess United States National Security Space Management and Organization (2001) Committee on armed services of the U.S. House of representatives, January 11, p 13. [https://fas.org/spp/military/commission/executive\\_summary.pdf](https://fas.org/spp/military/commission/executive_summary.pdf). Accessed 2 Apr 2019
- Sadeh E (2015) Obstacles in international space governance. In: Schrogl K-U et al (eds) Handbook of space security: policies, applications and programs. Springer, New York
- Sheehan M (2010) Rising powers: competition and cooperation in the New Asian space race. RUSI J 155(60):44
- Space Policy Directive-3, National Space Traffic Management Policy (2019) White House. <https://www.whitehouse.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy>. Accessed 10 Apr 2019
- The U.S. Anti-Satellite (ASAT) Program (1987) The U.S. Anti-Satellite (ASAT) program: a key element in the national strategy of deterrence. The White House, May 11. <https://fas.org/spp/military/program/asat/reag87.html>. Accessed 1 Apr 2019
- Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (1967) Opened for signature January 27. <http://www.oosa.unvienna.org/pdf/publications/STSPACE11E.pdf>. Accessed 1 Apr 2019
- Ullah S, Imam I (2019) What to make of India’s ASAT test. South Asian Voices, April 1. <https://southasianvoices.org/what-to-make-of-indias-asat-test/>. Accessed 2 Apr 2019
- Zervos V (2011) Conflict in space. In: Braddon L, Hartley K (eds) Handbook on the economics of conflict. Edward Elgar Publishing Limited, Northampton, p 215
- Zhang H (2008) Chinese perspectives on space weapons. In: Russian and Chinese responses to U.S. military plans in space. American Academy of Arts and Sciences, Cambridge, MA, p 31



# Spacepower Theory and Organizational Structures

# 4

Peter L. Hays

## Contents

Introduction .....	50
Noteworthy Efforts to Develop Spacepower Theory .....	51
Spacepower Theory and Current US Space Policy .....	56
Spacepower Theory, Hard Power, and the Quest for Sustainable Security .....	59
Spacepower Theory, Harvesting Energy, and Creating Wealth in and from Space .....	65
Spacepower Theory, Environmental Sustainability, and Survival .....	69
Conclusions .....	71
References .....	71

## Abstract

Spacepower theory is useful in describing, explaining, and predicting how individuals, groups, and states can best derive utility, balance investments, and reduce risks in their interactions with the cosmos. Spacepower theory should be more fully developed and become a source for critical insights as humanity wrestles with our most difficult and fundamental space challenges. This theory can help to guide us toward better ways to generate wealth in space, make tradeoffs between space investments and other important goals, reorder terrestrial security dynamics as space becomes increasingly militarized and potentially weaponized, and seize exploration and survival opportunities that only space can provide. This chapter reviews noteworthy efforts to develop spacepower theory and overviews recent changes in US organizational structures for spacepower. It then considers ways

---

The opinions expressed in this chapter are mine and do not imply endorsement by the Space Policy Institute, Falcon Research, or Department of Defense.

---

P. L. Hays (✉)

Space Policy Institute, George Washington University, Washington, DC, USA

e-mail: [hayspl@gwu.edu](mailto:hayspl@gwu.edu)

theory and structures could help to refine current US space policy and address some of the most significant challenges and issues surrounding space security, space commercialization, and environmental sustainability and survival.

---

## Introduction

The goal of spacepower theory is to describe, explain, and predict how individuals, groups, and states can best derive utility, balance investments, and reduce risks in their interactions with the cosmos. These are long-term, broad, indeterminate, and ambitious goals – it is hardly surprising that more than 60 years into the space age humanity has yet to develop spacepower theory able to address these goals in comprehensive and accepted ways. Incomplete and immature theory inhibits our ability to identify, pursue, and sustain major space objectives. More mature spacepower theory would provide critical insights as humanity wrestles with our most difficult and fundamental space challenges and guide us toward better ways to generate wealth in space, make tradeoffs between space investments and other important goals, reorder terrestrial security dynamics as space becomes increasingly militarized and potentially weaponized, and seize exploration and survival opportunities that only space can provide. This chapter reviews noteworthy efforts to develop spacepower theory and overviews recent changes in US organizational structures for spacepower. It then considers ways theory and structure could help to refine current US space policy and address some of the most significant challenges and issues surrounding space security, space commercialization, and environmental sustainability and survival.

Current perceptions that more robust spacepower theory is needed are undoubtedly most acute in the United States, but they are also growing worldwide as space becomes an increasingly contested and important domain. For decades, space capabilities gave the United States important asymmetric advantages that provided foundational elements of America's strength in the information age. These advantages are now being undermined by many factors including the reemergence of great power competition, the rise of China as a near-peer competitor with significant space and counterspace capabilities, continuing growth in the numbers and capabilities of space actors, and US uncertainties and missteps in determining and implementing its best strategy for developing and employing space capabilities. The trajectory of spacepower development has reached an inflection point where business as usual will no longer improve or even maintain US advantages – a point where the United States must implement different approaches or face diminishing returns from its space investments and the loss of space leadership. Attempting to identify and act upon inflection points is associated with strategic thinking and concepts of operations for terrestrial military operations; these approaches now hold obvious appeal to Americans pondering their space future. More mature and robust spacepower theory could help provide a more broad and stable foundation for the United States to develop a more deliberate, comprehensive, long-term, and consistent space strategy that would draw on all instruments of power from all levels of government, foster

unity of effort in national space activities, improve the viability of the US space industrial base, and, in particular, craft better ways to leverage state-of-the-world commercial and international space capabilities.

Despite its importance, movement toward developing better spacepower theory is likely to be slowed by discouraging attributes associated with spacepower that include lack of acceptance that such theory is needed, very large investments and long timelines, requirements for sustained popular and political support, and prospects for only potential or intangible benefits. These factors can erode acceptance of and support for improving spacepower theory at both the personal and political levels, but they also point to the need for an incremental approach and reinforce the long-term benefits of theory in providing guidance, stability, and predictability. Indeed, more robust spacepower theory could provide an essential foundation for improving the structure and predictability of humanity's interactions with the cosmos. Perhaps more than any other approach, the issues spacepower theory addresses, the precedents from which it is drawn, and the pathways ahead it helps to illuminate could help guide the future development of spacepower.

---

### **Noteworthy Efforts to Develop Spacepower Theory**

Many studies touch on aspects of spacepower theory, but few focus solely on this topic, and fewer still address the topic comprehensively and have widespread acceptance. This section briefly considers some of the most noteworthy efforts as well as elements of major and enduring themes and analogies any robust spacepower theory would need to address. The first major, comprehensive, and focused effort to develop spacepower theory began in 1997 when the Commander of US Space Command, General Howell M. Estes III, commissioned Dr. Brian R. Sullivan to write a book on this topic. James Oberg then became the leader of the effort and he published *Space Power Theory* in 1999 (Oberg 1999). Oberg draws on his academic background in astrodynamics and computer science as well as more than 20 years' experience with the National Aeronautics and Space Administration (NASA) Space Shuttle program to present a cogent narrative about the importance of spacepower that is particularly strong on the technical underpinnings of spacepower and emphasizes the need for space control. The book provides a strong foundation for spacepower theory, details the range of elements that contribute to its development, reviews how major space-faring states developed and used spacepower, and discusses several significant technical and political impediments to its development. Unfortunately, the political dimension of Oberg's spacepower theory is less well developed, primarily because his analysis does not provide much focus on the ways the attributes of spacepower relate to strategy or the development and employment of power in other domains.

By contrast, Everett Dolman, a professor in the Schriever Scholars program and at the School of Advanced Air and Space Studies at Air University, provides a spacepower theory that is focused almost entirely on the political rather than technical aspects of spacepower. *Astropolitik: Classical Geopolitics in the Space*

*Age* (Dolman 2001) explains how the physical attributes of outer space and the characteristics of space systems shape the application of spacepower and then uses this *astropolitical* analysis to develop a compelling vision for the United States to reject the Outer Space Treaty (OST) regime, promote free-market capitalism in space, and use space to help provide global security as a public good. His book is intellectually grounded in the best traditions of geopolitics, has something genuinely new to say, makes vital contributions to the dialogue about the interrelationships between space and national security, and is easily the most important book on space and security since the publication of Walter A. McDougall's Pulitzer prize-winning . . . *the Heavens and the Earth: A Political History of the Space Age* in 1985. *Astropolitik* is a stunning intellectual achievement and the first book that can legitimately claim to present a comprehensive theory of spacepower. It challenges conventional thinking about the status quo for space and has generated a great deal of controversy and provoked many responses. To be sure, many of the major points Dolman asserts are open to debate, such as whether space will actually become a virtually limitless source of wealth, what technologies and strategies the United States might employ to assert dominance over low-Earth orbit (LEO), and how and why domestic and international political forces might come to align with his astropolitical prescriptions. But one mark of a great book is that it helps to define and structure subsequent debate; *Astropolitik* has clearly advanced the study of spacepower theory by providing the language and lines of argumentation for future discourse.

There are several other noteworthy additions to this field: M. V. Smith's *Ten Propositions Regarding Spacepower*, John J. Klein's *Space Warfare: Strategy, Principles and Policy*, the National Defense University's (NDU) edited volume *Toward a Theory of Spacepower: Selected Essays*, and Klein's *Understanding Space Strategy: The Art of War in Space* (Smith 2001; Klein 2006, 2019; Lutes et al. 2011; Klein 2019). *Ten Propositions Regarding Spacepower* is written from the perspective of an Air Force officer who spent several years integrating space-related capabilities into numerous exercises and real-world combat; the study seeks to answer the philosophical question "what is the nature of spacepower?" Smith describes the nature of spacepower by presenting ten propositions, supporting each with historical evidence: Space is a distinct operational medium; the essence of spacepower is global access and global presence; spacepower is composed of a state's total space activity; spacepower must be centrally controlled by a space professional; spacepower is a coercive force; commercial space assets make all actors space powers; spacepower assets form a national center of gravity; space control is not optional; space professionals require career-long specialization; and weaponizing space is inevitable. Smith's propositions build from and are consistent with main themes in Oberg's and Dolman's works, but they independently advance spacepower theory by providing a more comprehensive and thorough exposition of the attributes of spacepower and its employment.

John J. Klein is a naval aviator, his books build from Carl von Clausewitz and other classic military theorists. In particular, Klein modifies for space the classic maritime theory presented by Julian Corbett in *Some Principles of Maritime Strategy* and first published in 1911. Corbett's theory about maritime activity is among the

best developed and comprehensive of all theories designed to explain military operations in terrestrial domains. Klein assesses airpower, seapower, and maritime strategies, finding that maritime strategy is most suitable for application to space; builds from Alfred Thayer Mahan's and Corbett's ideas about sea lines of communications to discuss the importance of celestial lines of communications; and asserts that there is an overemphasis on power and offensive space operations in current American spacepower thought. Klein's work advances spacepower theory by creating tight linkages with Corbett's well-developed maritime theory and providing a firm foundation for further refining spacepower theory.

The NDU spacepower theory study was commissioned by the Department of Defense (DoD) as the result of deliberations during preparation of the 2005 Quadrennial Defense Review. The study was a team effort to produce an edited volume and does not attempt to present a single point of view about spacepower theory. Instead, the study published 30 chapters written by national and international space experts and organized into six sections: introduction to spacepower theory; economics and commercial space perspectives; civil space perspectives; national security space perspectives; international perspectives; and evolving futures for spacepower. The strength of this approach is that it presents the most broad and wide-ranging perspectives ever assembled about spacepower theory, but weaknesses also stem from this approach, because there is no unified perspective or even many major common themes that emerge from the work. The overarching goal of the study was to foster dialogue and incubate further development of spacepower theory; it is hoped that the study's broad and wide-ranging perspectives will encourage advancement of spacepower theory along multiple paths.

Major and enduring themes and analogies any robust spacepower theory should address include perspectives on the growing use and importance of space, debates about the economic potential of space, debates over the need for and inevitability of space weaponization, perspectives of space as a frontier to be tamed, and perspectives that link space to humanity's purpose and destiny. Another set of factors shaping spacepower theory are the oft-invoked analogies between spacepower and seapower or airpower. Seminal theorists who developed important perspectives on sea and air operations include Mahan, Corbett, Giulio Douhet, William "Billy" Mitchell, and John Warden. (Several of these individuals were quite prolific; the following list represents their best known works: Mahan (1890), Corbett (1988), Douhet (1983), Mitchell (1988), and Warden (1988). On the importance of these works see Sumida (1997), Meilinger (1997), and Mets (1999).) Some of the key concepts that these theorists developed or applied to the air and sea mediums are command of the sea, command of the air, sea lines of communication, common routes, choke points, harbor access, concentration and dispersal, and parallel attack. Several of these concepts have been appropriated directly into various strands of embryonic space theory; others have been modified slightly and then applied. For example, Mahan's and Corbett's ideas about lines of communications, common routes, and choke points have been applied quite directly onto the space medium. Seapower and airpower concepts that have been modified to help provide starting points for thinking about spacepower include harbor access and access to space and

command of the sea or air and space control. But, of course, to date, no holistic spacepower theory has yet emerged that is fully worthy of claiming a place alongside the seminal seapower and airpower theories listed above. There are also many fundamental questions concerning the basic attributes of the space medium and how appropriate it is to analogize directly from seapower or airpower theory when attempting to build spacepower theory. Few concepts from seapower theory translate directly into airpower theory, and it is not reasonable to expect either seapower or airpower theory to apply directly for the distinct space domain.

Organizational structures also play a critical role in shaping US spacepower. Creation of the US Space Force (USSF) in December 2019 marks a momentous change in the structure of the US military and a significant shift in American strategic thought about the military utility of space (National Defense Authorization Act 2019). While this development alone cannot resolve all spacepower theory and space strategy issues, it may end an era of more than 30 years when the US was not satisfied with how it organized its national security space activities and churned through several different structures. Yet, because organizational structure is only a second-order issue, deeper questions remain related to the lack of consensus and direction on US objectives and priorities for its spacepower theory. The United States has yet to focus enough or reach consensus even domestically, let alone internationally, on first-order issues such as the long-term viability of the Outer Space Treaty (OST) regime, space weaponization, options for exploiting space resources and creating wealth in and from space, or other overarching issues related to the objectives it seeks from space, why these are important, and what the best strategies are to pursue these objectives. Worse, far too much current attention has been diverted toward third-order issues such as in which congressional districts Space Force units should be located or even what the Space Force patch and uniforms should look like. These are all issues and decisions that deserve some level of attention and hold some importance, but, as it stands up its first new military branch in more than 70 years, it is critical for the United States to focus initially on the first-order issue of the spacepower theory that will prioritize what the Space Force should do. Focusing on the organizational structure of the Space Force and first-order priorities for space can help the United States ask the right questions and move toward doing the right things, at the right times, and for the right reasons.

For the past several years, the United States was not able to reach consensus on the need for a Space Force, Space Corps, or other potential major reorganizations. Between 2017 and 2019, the House of Representatives and Senate Armed Services Committees were unable to reach a compromise on the Space Force. Elevating the issue above these committees in the fall of 2019 during budget negotiations allowed broader compromises between the parental leave provisions some Democrats wanted and Space Force provisions the President and some Republicans wanted. Unfortunately, expansion of the scope for compromises on a new organization did not extend beyond considering only a very narrow slice of military structure options or even the name of the new organization – the President insisted it be called the Space Force. The new Space Force resulting from these uncertainties and

compromises holds significant potential but faces continuing disagreements about its most important and appropriate near-term priorities and, as a military organization, is limited in its ability to effectively address the full range of first-order strategic space issues the United States currently faces. Another reflection of congressional concerns about the Space Force is the unprecedented level of oversight and reporting requirements Congress has levied on the new organization, including bi-monthly reporting on progress in establishing the Space Force.

There are several important concepts that can help us examine the Space Force and determine where it fits in relation to previous models and structures. Aristotle originated the idea that “form follows function,” a broad philosophical construct that includes deliberations on how organizational functions ought to determine organizational structure. This concept, along with Clausewitz’s assessments about inflection and culminating points, may be helpful as we consider the development of spacepower and how organizational structures may need to evolve. Another consideration for framing discussions on the Space Force is the adage that “when all you have is a hammer, everything looks like a nail” and the potential consequences of the United States choosing this military organization model and discussing the need for space dominance. Unlike most other national security mission areas, during the past 30 years, the Pentagon was directed to or chose itself to make several significant changes in its national security space organizational structures including the Deputy Under Secretary of Defense for Space (1994–1997); National Security Space Architect (1998–2004); National Security Space Office (2004–2010); Department of Defense (DoD) Executive Agent for Space (2003–2015); and Principal DoD Space Advisor (2015–2018). In addition, Air Force Space Command was established in 1982 and redesignated as the Space Force under the 2019 Space Force Act; and US Space Command was established in 1985, merged underneath US Strategic Command in 2002, and reestablished as an independent geographic combatant command in 2019.

The Space Force Act gives DoD 18 months to establish the initial operational capability of the Space Force and implement several other key provisions. The Act established the Space Force, a distinct armed force within the Department of the Air Force under the Secretary of the Air Force, and created a new General Officer position, the Chief of Space Operations (CSO). On 14 January 2020, Vice President Mike Pence administered the oath of office to Air Force General John “Jay” Raymond, making Raymond the first CSO and first member of the Space Force. The CSO is already attending meetings of the Joint Chief of Staff (JCS) and under the Act becomes a member of the JCS on 20 December 2021. The Space Force must establish its headquarters along with determining its subordinate units and their basing locations. All Space Force units will initially come from the Air Force, but, over time, it is expected that some Army and Navy units, along with appropriate Guard and Reserve units, will also transfer to the Space Force. Likewise, officers and enlisted personnel, initially from the Air Force, can voluntarily transfer into the Space Force. It is expected that some officers and enlisted personnel from the other Services, along with new accessions to the military, will also volunteer for the Space Force. Other key provisions in the Space Force Act establish a new Assistant



Secretary of the Air Force for Space Acquisition and Integration (ASecAF SA&I) position and a new Space Force Acquisition Council (SFAC). The ASecAF SA&I is a Senate-confirmed position that serves as the senior architect for space systems and programs across the Department of the Air Force, chairs the SFAC, is to become the Air Force Service Acquisition Executive (SAE) for space systems and programs as of 1 October 2022, and provides fiscal and strategic guidance by overseeing and directing the Space Rapid Capabilities Office, the Space and Missile Systems Center, and the Space Development Agency. The SFAC is to meet monthly, and its membership includes the Under Secretary of the Air Force, the Assistant Secretary of Defense for Space Policy, the Director of the National Reconnaissance Office (NRO), the CSO, and the Commander of the US Space Command.

---

## **Spacepower Theory and Current US Space Policy**

The United States has the most developed, open, and mature process for promulgating national space policy, and these space policies contain many elements that would be needed in robust and comprehensive spacepower theory. This is not to suggest that US space policy is the same as or can substitute for spacepower theory, but it does mean that attempts to develop spacepower theory need to be aware of and interact with these elements of US space policy. Widely accepted and comprehensive spacepower theory could help the United States refine its space policy, provide a stronger and more sustainable and consistent foundation for its implementation, and also improve its strategic-level management and organizational structures for implementing goals from the National Security Strategy, National Defense Strategy (NDS), and National Strategy for Space (NSfS).

The Trump Administration's National Security Strategy, released in December 2017, established America's vital national interest in space, reemphasized the importance of space for US security, and provided several overarching yet demanding objectives that will require focused attention and considerable effort to pursue:

The United States must maintain our leadership and freedom of action in space. Communications and financial networks, military and intelligence systems, weather monitoring, navigation, and more have components in the space domain. As U.S. dependence on space has increased, other actors have gained access to space-based systems and information. Governments and private sector firms have the ability to launch satellites into space at increasingly lower costs. The fusion of data from imagery, communications, and geolocation services allows motivated actors to access previously unavailable information. This "democratization of space" has an impact on military operations and on America's ability to prevail in conflict.

Many countries are purchasing satellites to support their own strategic military activities. Others believe that the ability to attack space assets offers an asymmetric advantage and as a result, are pursuing a range of anti-satellite (ASAT) weapons. The United States considers unfettered access to and freedom to operate in space to be a vital interest. Any harmful interference with or an attack upon critical components of our space architecture that directly affects this vital U.S. interest will be met with a deliberate response at a time, place, manner, and domain of our choosing.

#### Priority Actions

**ADVANCE SPACE AS A PRIORITY DOMAIN:** America’s newly re-established National Space Council, chaired by the Vice President, will review America’s long-range space goals and develop a strategy that integrates all space sectors to support innovation and American leadership in space.

**PROMOTE SPACE COMMERCE:** The United States will simplify and update regulations for commercial space activity to strengthen competitiveness. As the U.S. Government partners with U.S. commercial space capabilities to improve the resiliency of our space architecture, we will also consider extending national security protections to our private sector partners as needed.

**MAINTAIN LEAD IN EXPLORATION:** To enable human exploration across the solar system and to bring back to Earth new knowledge and opportunities, we will increase public-private partnerships and promote ventures beyond low Earth orbit with allies and friends. (National Security Strategy 2017)

Then Secretary of Defense James Mattis released an unclassified summary of the NDS in January 2018. The strategy sets three overarching objectives for DoD to address the reemergence of great power competition: rebuilding military readiness to develop a more lethal Joint Force, strengthening alliances and attracting new partners, and reforming DoD’s business practices for greater performance and affordability. The NDS designates space as a “warfighting domain” and indicates DoD will “prioritize investments in resilience, reconstitution, and operations to assure our space capabilities” (National Defense Strategy 2018).

In March 2018, the White House released the National Strategy for Space. The strategy established four pillars for a unified approach:

- Transform to more resilient space architectures: We will accelerate the transformation of our space architecture to enhance resiliency, defenses, and our ability to reconstitute impaired capabilities.
- Strengthen deterrence and warfighting options: We will strengthen U.S. and allied options to deter potential adversaries from extending conflict into space and, if deterrence fails, to counter threats used by adversaries for hostile purposes.
- Improve foundational capabilities, structures, and processes: We will ensure effective space operations through improved situational awareness, intelligence, and acquisition processes.
- Foster conducive domestic and international environments: We will streamline regulatory frameworks, policies, and processes to better leverage and support U.S. commercial industry, and we will pursue bilateral and multilateral engagements to enable human exploration, promote burden sharing and marshal cooperative threat responses. (National Strategy for Space 2018, p. 2)

Cumulatively, these documents move the Trump Administration considerably beyond the space policy of the Obama Administration. They reflect the “America First” more unilateral tone of many Trump Administration policies and move away from the stress on cooperation and responsible behavior in space in the 2010 National Space Policy. More specifically, the Trump Administration rejected the Obama Administration’s categorization of space stability and sustainability as vital national interests and returned to the previous approach that categorized just national security considerations as vital national interests in space as found in the 2006 and previous National Space Policies.

Additionally, the United States must continue to implement the many approaches and comprehensive actions detailed in the National Security Space Strategy (NSSS). The NSSS was signed by the Secretary of Defense and Director of National Intelligence and released in February 2011 (Secretary of Defense and Director of National Intelligence 2011). The NSSS publicly substantiated that space is growing increasingly congested, contested, and competitive: DoD is tracking over 22,000 man-made objects in space (including 1,100 active satellites), there are hundreds of thousands of additional debris pieces too small to track with current sensors but that could still damage satellites in orbit, and there is also increasing congestion in the radiofrequency spectrum due to satellite operations by more than 60 states and consortia and as many as 9,000 satellite communications transponders expected to be in orbit by 2012 (Secretary of Defense and Director of National Intelligence 2011, pp. 1–2).

Space is increasingly *contested* in all orbits. Today space systems and their supporting infrastructure face a range of man-made threats that may deny, degrade, deceive, disrupt, or destroy assets. Potential adversaries are seeking to exploit perceived space vulnerabilities. As more nations and non-state actors develop counterspace capabilities over the next decade, threats to US space systems and challenges to the stability and security of the space environment will increase. Irresponsible acts against space systems could have implications beyond the space domain, disrupting worldwide services upon which the civil and commercial sectors depend (Secretary of Defense and Director of National Intelligence 2011, p. 3).

And with respect to increasing competition, while the United States “maintains an overall edge in space capabilities,” its “competitive advantage has decreased as market-entry barriers have lowered”; its “technological lead is eroding in several areas”; “US suppliers, especially those in the second and third tiers, are at risk due to inconsistent acquisition and production rates, long development cycles, consolidation of suppliers under first-tier prime contractors, and a more competitive foreign market”; and the US share of world satellite manufacturing revenue has dropped from an average of more than 60% during the 1990s to 40% or less during the 2000s (Secretary of Defense and Director of National Intelligence 2011).

To address these challenges, the NSSS seeks three strategic objectives: strengthening safety, stability, and security in space; maintaining and enhancing the strategic national security advantages afforded to the United States by space; and energizing the space industrial base that supports US national security (Secretary of Defense and Director of National Intelligence 2011, p. 4). The strategy advocates five strategic approaches to pursue these objectives: promoting responsible, peaceful, and safe use of space; providing improved US space capabilities; partnering with responsible nations, international organizations, and commercial firms; preventing and deterring aggression against space infrastructure that supports US National Security; and preparing to defeat attacks and to operate in a degraded environment (Secretary of Defense and Director of National Intelligence 2011, pp. 5–11). Pursuit and implementation of these strategic objectives has proven challenging, but the NSSS correctly assesses the most significant changes in the space strategic environment and presents a responsible way for the United States to address these changes that begins to approach the comprehensive advances needed for spacepower theory.

## **Spacepower Theory, Hard Power, and the Quest for Sustainable Security**

There are several of hard power issue areas where spacepower theory might provide insights on space security including the OST regime and other transparency- and confidence-building measures (TCBMs), space situational awareness (SSA), space weaponization, and the rise of China as a major factor in space security. The OST regime is by far the most important and comprehensive mechanism in shaping space security. Although there is some substance to arguments that the OST only precludes those military activities that were of little interest to the superpowers and does not bring much clarity or direction to many of the most important potential space activities, the treaty nonetheless provides a solid and comprehensive starting point for spacepower theory and is an important foundation for thinking about additional theoretical structures needed to advance spacepower. Moreover, there is broad consensus on the merits and overall value of the OST regime; space-faring actors are much more interested in building upon this foundation than in developing new structures.

Spacepower theory should provide guidance on the most effective ways to confront the OST regime. Some theories would advocate abandoning this regime; most others would seek ways to improve and build upon the OST regime including working toward achieving more universal adherence by all space-faring actors to the regime's foundational norms and expanding the regime beyond just states to include all important space-faring actors. Beginning work to include major non-state space actors in the OST would be a significant step that would require substantial expansion of the regime and probably would need to be accomplished incrementally. The security dimensions of the regime have opened windows of opportunity, and important precedents have been set by expanding participation in the United Nations Committee on the Peaceful Uses of Outer Space (UN COPUOS) and the World Radio Conferences of the International Telecommunications Union (ITU) to include non-state actors as observers or associate members. Some form of two-tiered participation structure within the OST regime might be appropriate for a number of years, and it could prove impractical to include non-state actors in a formal treaty, but steps toward expanded participation should be carefully considered, both to capture the growing spacepower of non-state actors and to harness their energy in helping achieve more universal adherence to the regime. Perhaps most importantly, these initial steps would help promote a sense of stewardship for space among more actors and increase attention on those parties that fail to join or comply with these norms. Other particular areas within the OST regime that spacepower theory should address, perhaps through creation of a standing body with specific implementation responsibilities, include the Article VI obligations for signatories to authorize and exercise continuing supervision over space activities and the Article IX responsibilities for signatories to undertake or request appropriate international consultations before proceeding with any activity or experiment that would cause potentially harmful interference.

Another key area for security and spacepower theory for the United States and other leading space-faring actors that would help better define OST implementation

obligations and demonstrate leadership in fostering cooperative spacepower would be improvements in how SSA data is developed and shared globally. Due to increasing use of space by more actors, the growing number of active satellites, and, especially, recent deliberate and accidental debris creating events caused by the Chinese ASAT test in January 2007, the February 2009 collision between Iridium and Cosmos satellites, and the Indian ASAT test in March 2019, there is now more worldwide interest in spaceflight safety and considerable motivation for improvements in developing and sharing SSA data with more users in more timely and consistent ways. As a result of the 11 January 2007 Chinese ASAT test, the US Space Surveillance Network has cataloged 2,378 pieces of debris with diameters greater than 5 cm, is tracking 400 additional debris objects that are not yet cataloged, and estimates the test created more than 150,000 pieces of debris larger than 1 cm<sup>2</sup>. Unfortunately, less than 2% of this debris has reentered the atmosphere so far, and it is estimated that many pieces will remain in orbit for decades and some for more than a century (NASA Orbital Debris Program Office 2009).

Spacepower theory should provide guidance on the most effective approaches toward achieving these objectives. One approach would be continuation and improvements in US Government efforts to create a data center for sharing SSA data globally including ephemeris, propagation data, and pre-maneuver notifications for all active satellites. SSA issues are framed by specialized concepts and jargon. Conjunctions are close approaches, or potential collisions, between objects in orbit. Propagators are complex modeling tools used to predict the future location of orbital objects. Satellite operators currently use a number of different propagators and have different standards for evaluating and potentially maneuvering away from conjunctions. Maneuvering requires fuel and shortens the operational life of satellites. Orbital paths are described by a set of variables known as ephemeris data; two-line element sets (TLEs) are the most commonly used ephemeris data. Much of this data is contained in the form of a satellite catalog. The United States maintains a public catalog at [space-track.org](http://space-track.org). Other entities maintain their own catalogs. Orbital paths constantly change, or are perturbed, by a number of factors including Earth's inconsistent gravity gradient, solar activity, and the gravitational pull of other orbital objects. Perturbations cause propagation of orbital paths to become increasingly inaccurate over time; beyond approximately four days into the future, predictions about the location of orbital objects can be significantly inaccurate (Weeden 2009; McGlade 2007). Under Space Policy Directive-3, the Trump Administration is working to improve space traffic management and is planning to move the center for sharing SSA data globally from DoD to the Department of Commerce. Another approach would be to transition and operate such a data center under international auspices and perhaps create an international space traffic management organization that would be somewhat analogous to the International Civil Aviation Organization (ICAO). A final approach would build from commercial efforts such as the Space Data Association and Commercial Space Operations Center to encourage the commercial sector, rather than governments, to play the leading role in providing SSA data globally. In each case, processes would need to be developed and refined for users to voluntarily contribute data to the center, perhaps through a Global

Positioning System (GPS) transponder on each satellite, and for spaceflight safety data to be constantly updated, freely available, and readily accessible so that it could be used by satellite operators to plan for and avoid conjunctions.

Spacepower theory should also address difficult legal, technical, and policy issues that inhibit progress on sharing SSA data that include bureaucratic inertia, liability, and proprietary concerns; nonuniform data formatting standards and incompatibility between propagators and other cataloging tools; and security concerns over exclusion of certain satellites from any public data. Some of these concerns could be addressed by working toward better cradle-to-grave tracking of all cataloged objects to help establish the launching state and liability; using opaque processes to exclude proprietary information from public databases to the maximum extent feasible; and indemnifying program operators, even if they provide faulty data that results in a collision, so long as they operate in good faith, exercise reasonable care, and follow established procedures.

Theories for operating in other domains and history suggest there are very important roles for militaries both in setting the stage for the emergence of international legal regimes and in enforcing the norms of those regimes once they emerge. Development of any TCBMs for space, such as rules of the road or codes of conduct, should draw closely from the development and operation of such measures in other domains such as sea or air. The international community should consider the most appropriate means of separating military activities from civil and commercial activities in the building of these measures, because advocating a single standard for how all space activities ought to be regulated or controlled is inappropriately ambitious and not likely to be helpful. DoD requires safe and responsible operations by warships and military aircraft, but they are not legally required to follow all the same rules as commercial traffic and sometimes operate within specially protected zones that separate them from other traffic. Moreover, operational security considerations dictate that these military forces often do not provide public information about their location and planned operations. More robust spacepower theory as well as full and open dialogue about these issues will help us develop space rules that draw from years of experience in operating in other domains and make the most sense for the unique operational characteristics of space.

Other concerns surround the implications of various organizational structures and rules of engagement for potential military operations in space. Spacepower theory should help us address key questions such as whether military space forces should operate under national or only international authority, who should decide when certain activities constitute a threat, and how such forces should be authorized to engage threats, especially if such engagements might create other threats or potentially cause harm to humans or space systems. Clearly, these and several other questions are very difficult to address and require careful international vetting well before the actual operation of such forces in space. In addition, we should consider the historic role of the Royal and US Navies in fighting piracy, promoting free trade, and enforcing global norms against slave trading, as well as the current international effort to combat piracy off the Horn of Africa. What would be analogous roles in space for the US military and other military forces today and in the future and how

might the United States and others encourage like-minded actors to cooperate on such initiatives? Attempts to create legal regimes or enforcement norms that do not specifically include and build upon military capabilities are likely to be divorced from pragmatic realities and ultimately frustrating efforts (Joseph DeSutter 2006).

Robust and comprehensive spacepower theory should also address the viability and utility of various top-down and bottom-up approaches to TCBMs. The OST regime was developed through top-down methods, but since that success, many factors have made this approach increasingly difficult. The most serious of these problems include disagreements over the proper forum, scope, and object for negotiations; basic definitional issues about what is a space “weapon” and how they might be categorized as offensive or defensive and stabilizing or destabilizing; and daunting concerns about whether adequate verification mechanisms can be found for any comprehensive and formalized TCBMs that would likely prohibit certain space activities while seeking to encourage others. These problems relate to a number of very thorny, specific issues such as whether the negotiations should be primarily among only major space-faring actors or more multilateral, what satellites and other terrestrial systems should be covered, and whether the object should be control of space weapons or TCBMs for space; the types of TCBMs which might be most useful (e.g., rules of the road or keep out zones) and how these might be reconciled with the existing space law regime; and verification problems such as how to address the latent or residual ASAT capabilities possessed by many dual-use or military systems or how to deal with the significant military potential of even a small number of covert ASAT systems.

New space system technologies, continuing growth of the commercial space sector, and new verification technologies interact with these existing problems in complex ways. Some of the changes would seem to favor TCBMs, such as better radars and optical systems for improved SSA, attribution, and verification capabilities; technologies for better space system diagnostics; and the stabilizing potential of redundant and distributed space architectures that create many nodes by employing larger numbers of hosted payloads and less expensive satellites. Many other trends, however, would seem to make space arms control and regulation even more difficult. For example, very small satellites are becoming increasingly capable and might be used as virtually undetectable active ASATs or passive space mines; proliferation of space technology has radically increased the number of significant space actors to include a number of non-state actors that have developed or are developing sophisticated dual-use technologies such as autonomous rendezvous and docking capabilities; satellite communications technology can easily be used to jam rather than communicate; and growth in the commercial space sector raises issues such as how quasi-military systems could be protected or negated and the unclear security implications of global markets for dual-use space capabilities and products.

There is disagreement about the relative utility of top-down versus bottom-up approaches to developing space TCBMs and formal arms control, but, following creation of the OST regime, the United States and many other major space-faring actors have tended to favor bottom-up approaches, a point strongly emphasized by US Ambassador Donald Mahley in February 2008: “Since the 1970s, five

consecutive U.S. administrations have concluded it is impossible to achieve an effectively verifiable and militarily meaningful space arms control agreement” (Ambassador Mahley 2008). Yet this assessment may be somewhat myopic since strategists need to consider not only the well-known difficulties with top-down approaches but also the potential opportunity costs of inaction and recognize when they may need to trade some loss of sovereignty and flexibility for stability and restraints on others. Because the United States has not tested a kinetic energy ASAT since September 1985 and has no program to develop a dedicated ASAT system, would it have been better to exchange the option to maintain this capability for pursuit of a global ban on testing kinetic energy ASATs, and would such a norm have produced a restraining effect on development and testing of the Chinese ASAT? This may have been a lost opportunity to pursue TCBMs but is a complex, multi-dimensional, and interdependent issue shaped by a variety of other factors such as inability to distinguish between ballistic missile defense and ASAT technologies, reluctance to limit technical options after the end of the Cold War, the emergence of new and less easily deterred threats, and the demise of the Anti-Ballistic Missile (ABM) Treaty.

To circumvent significant challenges with top-down approaches, there have been several attempts to make progress through primarily incremental, pragmatic, technical, and bottom-up steps. Examples of this approach include the December 2007 adoption by the United Nations General Assembly of the Inter-Agency Debris Coordination Committee (IADC) voluntary guidelines for mitigating space debris, work initiated by the European Union toward an International Code of Conduct for outer space activities, the Long-Term Sustainability of Space Activities effort at UN COPUOS, and the United Nations Group of Governmental Experts on TCBMs (Council of the European Union 2008; United Nations General Assembly Resolution 62/217 2008).

Moreover, the Chinese, in particular, apparently disagree with pursuing only bottom-up approaches and, in ways that seem both shrewd and hypocritical, are currently developing significant counterspace capabilities while simultaneously advancing various top-down proposals in support of prevention of an arms race in outer space (PAROS) initiatives and moving ahead with the joint Chinese-Russian draft treaty on Prevention of Placement of Weapons in Outer Space (PPWT) introduced at the Conference on Disarmament in 2008 and updated in 2014. Thus far, the Chinese have seemed quite disinterested in pursuing space TCBMs; they are moving further and faster than any previous spacefaring actor and in 2013 tested a dedicated high-altitude ASAT system able to hold geostationary satellites at risk, a capability never pursued by the superpowers at the height of the Cold War. With respect to the PPWT in particular, while it goes to considerable lengths in attempting to define space, space objects, weapons in space, placement in space, and the use or threat of force, there are still very considerable definitional issues with respect to how specific capabilities would be addressed. An even more significant problem relates to all the terrestrial capabilities that could eliminate, damage, or disrupt normal functioning of objects in outer space such as the Chinese direct ascent ASAT. One must question the utility of a proposed agreement that does not address



the significant security implications of current space system support of network-enabled terrestrial warfare, does not deal with dual-use space capabilities, seems to be focused on a class of weapons that does not exist or at least is not deployed in space, is silent about all the terrestrial capabilities that are able to produce weapons effects in space, and would not even ban development and testing of space weapons, only their use (Reaching Critical Will, “Preventing the Placement of Weapons in Outer Space: A Backgrounder on the draft treaty by Russia and China”). Given these glaring weaknesses in the PPWT, it seems plausible that it is designed as much to continue political pressure on the United States and derail US missile defense efforts as it is to promote sustainable space security.

Since Sino-American relations in general and space relations in particular are likely to play a dominant role in shaping spacepower theory and the quest for sustainable security during this century, proposed Sino-American cooperative space ventures or TCBMs are worthy of special consideration. For example, the United States could make more specific and public invitations for the Chinese to become involved with the International Space Station program and join other major cooperative international space efforts. The United States and China could also work toward developing non-offensive defenses of the type advocated by Philip Baines (2003). Kevin Pollpeter explains how China and the United States could cooperate in promoting the safety of human spaceflight and “coordinate space science missions to derive scientific benefits and to share costs. Coordinating space science missions with separately developed, but complementary space assets, removes the chance of sensitive technology transfer and allows the two countries to combine their resources to achieve the same effects as jointly developed missions” (Pollpeter 2008). Michael Pillsbury outlined six other areas where US experts could profitably exchange views with Chinese specialists in a dialogue about space weapons issues: “reducing Chinese misperceptions of U.S. Space Policy, increasing Chinese transparency on space weapons, probing Chinese interest in verifiable agreements, multilateral versus bilateral approaches, economic consequences of use of space weapons, and reconsideration of U.S. high-tech exports to China” (Pillsbury 2007). Finally, Bruce MacDonald’s report on *China, Space Weapons, and U.S. Security* for the Council on Foreign Relations offers several noteworthy additional specific recommendations for both the United States and China. For the United States, MacDonald recommends: assessing the impact of different US and Chinese offensive space postures and policies through intensified analysis and “crisis games,” in addition to wargames; evaluating the desirability of a “no first use” pledge for offensive counterspace weapons that have irreversible effects; pursuing selected offensive capabilities meeting important criteria – including effectiveness, reversible effects, and survivability – in a deterrence context to be able to negate adversary space capabilities on a temporary and reversible basis, refraining from further direct ascent ASAT tests and demonstrations as long as China does, unless there is a substantial risk to human health and safety from uncontrolled space object reentry; and entering negotiations on a kinetic energy ASAT testing ban. MacDonald’s recommendations for China include providing more transparency into its military space programs; refraining from further direct ascent ASAT tests as long as the United States does;

establishing a senior national security coordinating body, equivalent to a Chinese National Security Council; strengthening its leadership's foreign policy understanding by increasing the international affairs training of senior officer candidates and establishing an international security affairs office within the People's Liberation Army; providing a clear and credible policy and doctrinal context for its 2007 ASAT test and counterspace programs more generally and addressing foreign concerns over China's ASAT test; and offering to engage in dialogue with the United States on mutual space concerns and become actively involved in discussions on establishing international space codes of conduct and confidence-building measures (MacDonald 2008).

---

### **Spacepower Theory, Harvesting Energy, and Creating Wealth in and from Space**

Moving from hard to soft power considerations, spacepower theory can help to guide spacefaring actors in a number of important areas including further developing and refining the OST regime, adapting the most useful parts of analogous regimes such as the Law of the Sea and Seabed Authority mechanisms, and rejecting standards that stifle innovation, inadequately address threats to humanity's survival, or do not provide opportunities for rewards commensurate with risks undertaken. Revising and further developing the OST regime could be a key first step toward seeking better ways to harvest energy and create wealth in and from space. Expanding participation in the OST as discussed above might also be helpful, but other steps such as reducing liability concerns and improving legal incentives for harvesting energy and generating wealth are likely to be even more effective in pursuit of further commercial development of space. Of course, as with security, more comprehensive and robust spacepower theory would be helpful in considering a range of objectives and values that are in tension and require considerable effort to change or keep properly balanced. The OST has been extremely successful thus far with respect to its primary objective of precluding replication of the colonial exploitation that plagued much of Earth's history. The international community should now consider whether the dangers posed by potential cosmic land grabs continue to warrant OST restrictions that stifle development of spacepower, and, if these values are found to have become imbalanced, how these restrictions might best be changed. Space-faring actors should use an expansive approach to consider how perceived OST restrictions and the commercial space sector have evolved and might be further advanced in a variety of ways including reinterpreting the OST regime itself, becoming more intentional about developing spacepower, creating space-based solar power capabilities, and improving export controls.

While the OST has thus far been unambiguous and successful in foreclosing sovereignty claims and the ills of colonization, it has been less clear and effective with respect to pragmatic property rights and commercialization issues. Part of the problem in this regard stems from the fact that OST is not linked to robust and mature spacepower theory; the regime is also embedded within a broader body of

international law and that regime is evolving, sometimes in unclear ways and under different interpretations. Elements within the regime are of unclear and unequal weight: the Moon Agreement with its Common Heritage of Mankind (CHM) approach to communal property rights and equally shared rewards has some effect but more limited standing as customary international law due to its lack of signatories, especially among major spacefaring states; moreover, it falls well short of the OST, a treaty that has been signed by 109 states and in force for over 50 years. Most fundamentally, however, the lack of clarity within space law about property rights and commercial interests is the result of the regime still being underdeveloped and immature. There is also a “Catch-22” factor at work since actors are discouraged from undertaking the test cases needed to develop and mature the regime because of the immaturity of the regime and their unwillingness to be guinea pigs in whatever legal processes would be used to resolve property rights and reward structures. The most effective way to move past this significant hurdle would be to create clear mechanisms for establishing property rights and processes by which all actors, especially commercial actors, can receive rewards commensurate with the risks they undertake. In addition, consideration should be given to reevaluating liability standards by assessing factors, including how much of a disincentive toward appropriate risk taking they may create and whether use of graduated or reduced liability standards might be more suitable in advancing positive incentives for more commercial space activity. Although Art. VII of the OST discusses liability, that article was further implemented in the Convention on International Liability for Damage Caused by Space Objects, commonly referred to as the Liability Convention. Under the Liability Convention, Article II, a launching state is absolutely liable to pay compensation for damage caused by its space object on the surface of the Earth or to aircraft in flight. However, under Articles III and IV, in the event of damage being caused elsewhere than on the surface of the Earth by a space object, the launching state is liable only if the damage is due to its fault or the fault of persons for whom it is responsible (i.e., commercial companies), under a negligence standard. The challenge is how best to evolve the existing space law regime with its two-tiered liability system based on either absolute liability or fault/negligence, depending upon the location of the incident, into a structure that might provide more incentives for commercial development of space (Convention on International Liability for Damage Caused by Space Objects (resolution 2777 (XXVI) annex)). In the Commercial Space Launch Act of 2015 and subsequent legislation, the US Congress indicated that US citizens “engaged in commercial recovery of an asteroid resource or a space resource under this chapter shall be entitled to any asteroid resource or space resource obtained, including to possess, own, transport, use, and sell the asteroid resource or space resource obtained in accordance with applicable law, including the international obligations of the United States.” Other states including Luxembourg and the United Arab Emirates have enacted similar legislation, but in all cases the details of how these domestic laws will be implemented and remain compliant with state obligations under the OST remain to be seen. Finally, any comprehensive reevaluation of space property rights and liability concerns should also consider how these factors are addressed in analogous regimes such as the

Seabed Authority in the Law of the Sea Treaty. Unfortunately, however, several of the analogous regimes like the Law of the Sea are largely premised on CHM approaches and may be somewhat better developed than the OST but are also currently underdeveloped and immature with respect to actual commercial operations, limiting the utility of attempting to draw from these precedents.

Provisions of the OST regime are probably the most important factors in shaping commercial space activity, but they are clearly not the only noteworthy legal and policy factors at work influencing developments within this sector. Commercial space activity was not that significant during the Cold War, but that has changed radically. In the 1960s, the United States was first to begin developing space services such as communications, remote sensing, and launch capabilities but did so within the government sector. This approach began to change in the 1980s, first with the November 1984 Presidential Determination to allow some commercial communication services to compete with Intelsat, and continued with subsequent policies designed to foster development of a commercial space sector. By the late 1990s, commercial space activity worldwide was outpacing government activity, and although government space investments remain very important, they are likely to become increasingly overshadowed by commercial activity. Other clear commercial and economic distinctions with the Cold War era have even more significant implications for the future of spacepower: the Soviet Union was only a military superpower, whereas China is a major US trading partner and an economic superpower that recently passed Germany and Japan to become the world's second largest economy and, if current growth projections hold, is on a path to become larger than the US economy by 2030. Because of its economic muscle, China can afford to devote commensurately more resources to its military, including a wide range of increasingly capable space and counterspace capabilities.

The United States and other major spacefaring actors lack, but undoubtedly need, much more open and comprehensive visions for how to develop spacepower theory and advance spacepower. This study is one attempt to foster more dialogue about space security, but the process should continue, become more formalized, and be supported by enduring organizational structures that include the most important stakeholders in the future of spacepower. Spacepower theory should be a foundational part of creating and implementing spacepower and guide approaches “focused on opening space as a medium for the full spectrum of human activity and commercial enterprise, and those actions which government can take to promote and enable it, through surveys, infrastructure development, pre-competitive technology, and encouraging incentive structures (prizes, anchor-customer contracts, and property/exclusivity rights), regulatory regimes (port authorities, spacecraft licensing, public-private partnerships) and supporting services (open interface standards, RDT&E [research, development, test, and evaluation] facilities, rescue, etc.)” (Garretson 2009). In addition, consideration should be given to using other innovative mechanisms and nontraditional routes to space development, including a much wider range of federal government organizations and the growing number of state spaceport authorities and other organizations developing needed infrastructure. Finally, the United States should make comprehensive and careful exploration of the potential of

space-based solar power its leading pathfinder in creating a vision for developing spacepower. Working toward harvesting this unlimited power source in economically viable ways will require development of appropriate supporting structures, particularly with respect to incentives, indemnification, and potential public-private partnerships.

Better spacepower theory should also provide guidance on better ways to implement global licensing and export controls for space technology. It is understandable that many states view space technology as a key strategic resource and are very concerned about developing, protecting, and preventing the proliferation of this technology, but the international community, and the United States in particular, needs to find better legal mechanisms to balance and advance objectives in this area. Many current problems with US export controls began after Hughes and Loral worked with insurance companies to analyze Chinese launch failures in January 1995 and February 1996. A congressional review completed in 1998 (Cox Report) determined these analyses violated the International Traffic in Arms Regulations (ITAR) by communicating technical information to the Chinese. The 1999 National Defense Authorization Act transferred export controls for all satellites and related items from the Commerce Department to the Munitions List administered by the State Department. The January 1995 failure was a Long March 2E rocket carrying Hughes-built Apstar 2 spacecraft, and the February 1996 failure was a Long March 3B rocket carrying Space Systems/Loral-built Intelsat 708 spacecraft. Representative Christopher Cox (R-California) led a 6-month-long House Select Committee investigation that produced the “U.S. National Security and Military/Commercial Concerns with the People’s Republic of China” Report released on 25 May 1999. In January of 2002, Loral agreed to pay the US government \$20 million to settle the charges of the illegal technology transfer, and in March of 2003, Boeing agreed to pay \$32 million for the role of Hughes (which Boeing acquired in 2000). Requirements for transferring controls back to State were in Sections 1513 and 1516 of the Fiscal Year 1999 National Defense Authorization Act. Related items were defined as “satellite fuel, ground support equipment, test equipment, payload adapter or interface hardware, replacement parts, and non-embedded solid propellant orbit transfer engines.” The stringent Munitions List controls contributed to a severe downturn in US satellite exports. To avoid these restrictions, foreign satellite manufacturers, beginning in 2002 with Alcatel Space (now Thales) and followed by European Aeronautic Defense and Space Company (EADS), Surrey Satellite Company, and others, replaced all US-built components on their satellites to make them “ITAR-free” (de Selding 2005; Barrie and Taverna 2006).

Following the recommendations for rebalancing overall US export control priorities in the congressionally mandated National Academies of Science (NAS) study (National Research Council 2009), the Center for Strategic and International Studies (CSIS) study on the space industrial base (Briefing of the working group on the health of the U.S. space industrial base and the impact of export controls 2008), and the congressionally mandated section 1248 report completed by the Departments of State and Defense that assessed risks associated with removing satellites and related components from the US Munitions List, both the Obama Administration

and Congress moved to reform US export controls in significant ways. The administration's proposal was advanced in August 2009 and called for "four singles": a single export control licensing agency for both dual-use and munitions exports, a unified control list, a single enforcement coordination agency, and a single integrated information technology (IT) system supporting the export control process. Following the significant space export control reforms enacted in 2014, the Trump Administration is looking toward additional export control reforms as well as streamlining efforts for other regulatory and licensing procedures under Space Policy Directive-2. These changes will help the United States avoid two major problems with an overly restrictive export control regime: First, an overly broad approach that tries to protect too many things dilutes resources and actually results in less protection for "crown jewels" than does a focused approach; and second, a more open approach is more likely to foster innovation, spur development of sectors of comparative advantage, and improve efficiency and overall economic growth.

---

## **Spacepower Theory, Environmental Sustainability, and Survival**

The area where insights from spacepower theory undoubtedly could help provide the most significant contributions would be in improving environmental sustainability and humanity's odds for survival. More mature and robust spacepower theory is needed, because advancements in these areas face many daunting challenges, including a high "giggle factor," very long timelines that can be beyond our political and personal awareness, and potential returns that are uncertain and intangible. While difficult, work in these areas is absolutely critical, since it may hold the key to humanity's very survival, and it must be pursued with all the resources, consistency, and seriousness it deserves. The quest to improve the ways spacepower theory can support environmental and survival objectives should focus in three areas: space debris, environmental monitoring, and planetary defense.

Human space activity produces many orbital objects; when these objects no longer serve a useful function, they are classified as space debris. Over time, human activity has generated an increasing amount of debris from a variety of causes; the number of cataloged debris objects has gone from about 8,000 to over 22,000 over the past 20 years. The most serious cause of debris is deliberate hypervelocity impacts between large objects at high orbital altitudes such as the Chinese direct ascent kinetic energy ASAT weapon test of January 2007. If current trends continue, there is growing risk that space, and LEO in particular, will become increasingly unusable. Fortunately, there is also growing awareness and earnestness across the international community in addressing this threat. Overall goals for spacefaring actors with respect to space debris include minimizing its creation while mitigating and remediating its effects – spacepower theory can play an important role in raising awareness and providing guidance in all these areas. Key approaches to minimizing creation of debris and mitigating against its effects are commercial best practices and evolving regimes such as the IADC voluntary guidelines. Space-faring actors need to consider mechanisms to transition these voluntary guidelines into more binding standards and ways to impose

specific costs such as sanctions or fines on actors that deliberately or negligently create long-lived debris. Fines could be applied toward efforts to further develop and educate spacefaring actors about the debris mitigation regime as well as to create, implement, and improve remediation techniques. An additional potential source of funding for mitigation and remediation would be establishing auctions for the radiofrequency spectrum controlled by the ITU that would be analogous to the spectrum auctions conducted at the national level by organizations like the Federal Communications Commission. Finally, it must be emphasized that techniques for remediating debris using lasers or other methods are likely to have significant potential as ASAT weapons, and very careful consideration should be given to how and by whom such systems are operated.

Space provides a unique location to monitor and potentially remediate Earth's climate. It is the only location from which simultaneous in situ observations of Earth's climate activity can be conducted and such observations are essential to develop a long-term understanding of potential changes in our biosphere. Because so much is riding on our understanding of the global climate and our potential responses to perceived changes, spacepower theory could play a particularly important role in helping us apply apolitical standards in getting the science right and controlling for known space effects such as solar cycles when making these observations and building climate models. If alarming models about global warming are correct and the global community must implement active measures to remediate these effects, space also provides a unique location to operate remediation options such as orbital solar shades, and space-based solar power has the potential to replace the use of some fossil fuels on Earth.

It is also imperative that the United States and all spacefaring actors use insights from spacepower theory and other sources to be more proactive, think more creatively, and transcend traditional approaches toward emerging threats to our survival. Spacepower theory can help to illuminate paths toward and develop incentives to create a better future. Space, perhaps more than any other medium, is inherently linked to humanity's future and very survival. We need to link these ideas together and better articulate ways spacepower can light a path toward genuinely cooperative approaches for protecting the Earth and space environments from cataclysmic events such as large objects that may collide with Earth or gamma ray bursts that have the potential to extinguish all life on Earth if we are unlucky enough to be in their path. Better knowledge about known threats such as near-Earth objects (NEOs) is being developed, but more urgency is required. The predicted near approach of the asteroid Apophis on 13 April 2029 ought to serve as a critical real-world test for our ability to be proactive in developing effective precision tracking and NEO mitigation capabilities. In the near term, it is most important for national and international organizations to be specifically charged with developing better understanding of NEO threats and developing avoidance techniques that can be effectively applied against likely impacts. Ultimately, however, as any robust and comprehensive spacepower theory would tell us, we cannot know of or effectively plan for all potential threats but should pursue multidimensional approaches to develop capabilities to improve our odds for survival and one day perhaps become a multi-planetary species.

## Conclusions

This chapter reviewed noteworthy efforts to develop spacepower theory, considered ways it could help to refine current US space policy, and used it to address some of humanity's most significant space challenges including space security, space commercialization, and environmental sustainability and survival. Spacepower theory can describe, explain, and predict how individuals, groups, and states can best derive utility, balance investments, and reduce risks in their interactions with the cosmos; it should be more fully developed and become a source for critical insights. It could help to guide us toward better ways to generate wealth in space, make tradeoffs between space investments and other important goals, reorder terrestrial security dynamics as space becomes increasingly militarized and potentially weaponized, and seize exploration and survival opportunities that only space can provide.

There will be inevitable missteps, setbacks, and unintended consequences, but the inexorable laws of physics and of human interaction indicate that we will create the best opportunities for success in advancing spacepower by beginning long-term, patient work now rather than a crash program later. Spacepower theory should provide an essential foundation for this progress.

---

## References

- Ambassador Mahley DA (2008) Remarks on the state of space security. In: The state of space security workshop, Space Policy Institute, George Washington University, Washington, DC
- Baines PJ (2003) The prospects for 'non-offensive' defenses in space. In: Moltz JC (ed) *New challenges in missile proliferation, missile defense, and space security*. Center for Nonproliferation Studies occasional paper no 12. Monterey Institute of International Studies, Monterey, pp 31–48
- Barrie D, Taverna MA (2006) Specious relationship. *Aviat Week Space Technol* 17:93–96
- Center for Strategic and International Studies (2008) Briefing of the working group on the health of the U.S. space industrial base and the impact of export controls. Center for Strategic and International Studies, Washington, DC
- Corbett JS (1988) In: Grove EJ (ed) *Some principles of maritime strategy*. Naval Institute Press, Annapolis (First published 1911)
- Council of the European Union (2008) Council conclusions and draft Code of Conduct for outer space activity. Council of the European Union, Brussels
- de Selding PB (2005) European satellite component maker says it is dropping U.S. components because of ITAR. *Space News Business report*, 13 June 2005
- Dolman EC (2001) *Astropolitik: classical geopolitics in the space age*. Routledge, New York
- Douhet G (1983) In: Kohn RH, Harahan JP (eds) *The command of the air*. Office of Air Force History, Washington, DC (First published 1921)
- Garretson P (2009) Elements of a 21st century space policy. *The Space Review*, 3 August 2009. Downloaded from <http://www.thespacereview.com/article/1433/1>
- Joseph DeSutter R (2006) Space control, diplomacy, and strategic integration. *Space Def* 1(1): 29–51
- Klein JJ (2006) *Space warfare: strategy, principles, and policy*. Routledge, New York
- Klein JJ (2019) *Understanding space strategy: the art of war in space*. Routledge, New York
- Lutes CD, Hays PL, Manzo VA, Yambrick LM, Bunn ME (eds) (2011) *Toward a theory of spacepower: selected essays*. National Defense University Press, Washington, DC



- MacDonald BW (2008) China, space weapons, and U.S. security. Council on Foreign Relations, New York, pp 34–38
- Mahan AT (1890) The influence of sea power upon history, 1660–1783. Little, Brown, Boston
- McGlade D (2007) Commentary: preserving the orbital environment. *Space News*, 19 February 2007, p 27
- Meilinger PS (ed) (1997) The paths of heaven: the evolution of airpower theory. Air University Press, Maxwell
- Mets DR (1999) The air campaign: John Warden and the classical airpower theorists. Air University Press, Maxwell
- Mitchell W (1988) Winged defense: the development and possibilities of modern airpower – economic and military. Dover, New York (First published 1925)
- NASA Orbital Debris Program Office (2009) Fengyun 1-C Debris: Two Years Later. *Orbital Debris Quarterly News* 13(1):2. Johnson Spaceflight Center: NASA Orbital Debris Program Office
- National Defense Authorization Act (NDAA) (2019) Conference report to accompany National Defense Authorization Act for fiscal year 2020. The Space Force Act is Sections 951–61 of the fiscal year (FY) 2020. US Congress. Washington, DC. <https://docs.house.gov/billssthisweek/20191209/CRPT-116hrpt333.pdf>
- National Defense Strategy (2018) Summary of the 2018 National Defense Strategy. Department of Defense, Washington, DC, p 6. <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>
- National Research Council (2009) Beyond “Fortress America”: national security controls on science and technology in a globalized world. National Academies Press, Washington, DC
- National Security Strategy (2017) The White House, Washington, DC, p 31. <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>
- National Strategy for Space (2018) The White House, Washington, DC, p 2. <https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy/>
- Oberg JE (1999) Space power theory. United States Space Command, Colorado Springs
- Pillsbury MP (2007) An assessment of China’s anti-satellite and space warfare programs, policies, and doctrines. Report prepared for the U.S.-China Economic and Security Review Commission, p 48
- Pollpeter K (2008) Building for the future: China’s progress in space technology during the tenth 5-year plan and the US response. Strategic Studies Institute, Carlisle Barracks, pp 48–50
- Secretary of Defense and Director of National Intelligence (2011) National security space strategy: unclassified summary. Office of the Secretary of Defense and Office of the Director of National Intelligence, Washington, DC
- Smith MV (2001) Ten propositions regarding spacepower. Air University Press, Maxwell
- Sumida JT (1997) Inventing grand strategy and teaching command: the classic works of Alfred Thayer Mahan reconsidered. Woodrow Wilson Center Press, Washington, DC
- United Nations General Assembly Resolution 62/217 (2008) International cooperation in the peaceful uses of outer space. UNGA, New York
- Warden JA III (1988) The air campaign: planning for combat. National Defense University Press, Washington, DC
- Weeden B (2009) The numbers game. *The Space Review*, 13 July 2009. Downloaded from <http://www.thespacereview.com/article/1417/1>



# The Laws of War in Outer Space

# 5

Steven Freeland and Elise Gruttner

## Contents

Introduction .....	74
General Principles of Space Law .....	75
Principles Regulating the “Military” Uses of Outer Space .....	80
The Laws of War: General Principles .....	82
Distinction .....	83
Military Objective .....	84
Proportionality .....	84
The Relevance of the Laws of War to Outer Space .....	85
Regulating the Threat of Space Warfare: Some Recent Initiatives .....	87
Conclusion: Perspectives on the Way Forward .....	89
References .....	91

## Abstract

With the development of technology accelerating at a rapid pace, there has not been a more crucial time to analyze the international legal framework of outer space. The use of outer space for armed conflict is now a reality for space-faring nations and, as such, attention needs to be placed on the legal implications of this modern (potential) theatre of warfare. The applicability of international law to outer space was confirmed in the United Nations Outer Space Treaty that applies to the use and exploration of outer space. With new technologies such as dual-use satellites emerging, complex international law issues relating to the use of force and understanding how and to what extent the international law principles of *jus in bello* – international humanitarian law – apply to the regulation of these outer

---

S. Freeland (✉)

University of Western Sydney, Sydney, NSW, Australia  
e-mail: [S.Freeland@westernsydney.edu.au](mailto:S.Freeland@westernsydney.edu.au)

E. Gruttner (✉)

United Nations Assistance to the Khmer Rouge Trials, New York, NY, USA  
e-mail: [elise.gruttner@gmail.com](mailto:elise.gruttner@gmail.com)

space activities. This chapter examines the evolution of outer space technology and the relevant legal frameworks that exist, and looks at certain aspects of the *jus in bello* principles that relate to the use of outer space. Some legal principles that exist in international humanitarian law may apply to activities in outer space; however, it remains unclear whether these principles are specific enough to take into account the increasingly diverse ways in which outer space could be utilized during the course of armed conflict. Consequently, there is a growing need for clarity in this evolving field of law, particularly as it relates to armed conflict in outer space.

---

## Introduction

It is now more than 60 years since humankind began its “adventures” in outer space. On 4 October 1957, a Soviet space object, Sputnik I, was launched and subsequently orbited the Earth. The launch of Sputnik I heralded the dawn of the space age, the beginning of the space race (initially between the USSR and the United States), and the legal regulation of the use and exploration of outer space. Since then, laws regulating outer space technology have developed which significantly improve the standard of living for all humanity, through, for example, the facilitation of public services such as satellite telecommunications, global positioning systems, remote sensing technology for weather forecasting and disaster management, and television broadcast from satellites. Outer space offers the opportunity for immense social, economic, and scientific growth; however, new challenges are being posed to humanity through this advancement, and law will continue to play a crucial role in this regard.

The commencement of the space age began at the height of the Cold War, when both the United States and the USSR strove to flex their respective technological “muscles.” At the time, the two leading space superpowers raced to develop their space capabilities, generating tension on a global scale. In October 1962, shortly after the launch of Sputnik I, the “Cuban Missile Crisis” threatened global security. This security-sensitive environment resulted in the international community’s first endeavors to regulate this new frontier of outer space. While the purpose was to reduce the build up of weapons in space, the conventional obligations and restrictions that were agreed upon and codified in the major space treaties were neither entirely clear nor sufficiently comprehensive to meet all of these challenges. While a large body of space scholars would interpret the relevant provisions as prohibiting military space activities in outer space, those who had the capability to use space technology did not follow these restrictions. Since that time, it is clear that space has been utilized for military activities almost from the time of the very infancy of space activities.

Since the commencement of outer space activities, the environment has become significantly more complex and the consequences have heightened. Through the use of remote satellite technology and communication technology, information is being gathered and constantly relied upon by all aspects of society. This information is also

an element in direct terrestrial military activity and represents an integral part of the major superpowers' respective military hardware. With outer space being increasingly used as part of active engagement in the conduct of armed conflict, it is now within the bounds of possibility to imagine outer space as an emerging theatre of warfare (Ricks 2001).

With the development of these outer space capabilities in mind, this chapter focuses on the potential application of the current laws of war to the use of outer space. While the last 60 years has shown us that outer space is being utilized for military purposes, it is not clear how these activities are treated and regulated at the international level. Through applying an analysis of the existing *jus in bello* principles to the domain of outer space, it would seem that the current capability of space-related technology exists outside the established international framework that has regulated the laws of war to date. The unique environment that outer space poses leaves some instances in which the established *jus in bello* principles application are not suitable as a regulatory system for the distinctive domain that is outer space.

Accordingly, this chapter will briefly outline the fundamental principles governing the international legal regulation of outer space and focus more specifically on those that are most relevant to military and warfare-related activities that utilize space technology. Subsequently, it examines the general principles that govern the laws of war in brief, before discussing these principles' relevance to outer space. Following on from this, a number of initiatives designed to (potentially) fill some of the lacunae that appear to exist within the current legal regime will be outlined, before we make some more general observations regarding the way forward in terms of legal regulation.

Ultimately, notwithstanding that the laws of war do theoretically apply to activities in outer space, the principles may not be specific enough to provide appropriate regulation for the increasingly diverse ways in which outer space could be used during the course of armed conflict. With the world's growing dependence on space technology and the ever-increasing space race among the major super powers, it is more important than ever to examine the existing international principles and reach a consensus on additional legal regulation directly applicable to the conduct of armed conflict in outer space. This will require close cooperation and greater trust between the major space powers, supported by other States and the international community. If this framework can be established, it may provide more certainty among the leading space-faring nations and could reduce the risk of the negative repercussions that are associated with space assets and activities.

---

## General Principles of Space Law

The launch of Sputnik I immediately gave rise to difficult and controversial legal questions, involving previously undetermined concepts. Early academia contemplated the nature and scope of laws that might apply to the exploration and use of outer space, but only at a hypothetical level (Lyall and Larsen 2009). The world has since moved on from mere contemplation and has entered a new age of space

technology and reliance. Humanity's ability to adapt and aspire to greater heights has led to the explosion of scientific exploration, the commercialization, and the militarization of outer space. With this rapid change came the international community's need to react to an unprecedented event of an unregulated legal environment.

These changes in space activities were largely driven at the time by the geopolitical situation – predominantly the state of Cold War that prevailed between the United States and the USSR. Time has shown us that the desire for ever-increasing technological prowess was as much motivated by military aspirations as a wish to explore and use space for other (scientific) purposes. It was in this conflicting environment that the international community had to respond. Between the desire of the two superpowers and the greater concerns among the international community, regulation had to somehow strike a balance between contrasting interests.

Accordingly, soon after the launch of Sputnik I, the United Nations established a new committee to take primary responsibility for the development and codification of the fundamental rules relating to the use and exploration of outer space with the name of United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS). An ad hoc Committee on the Peaceful Uses of Outer Space, with 18 initial Member States, was established in 1958 by the United Nations General Assembly (UNGA 1958), which subsequently converted it into a permanent body in 1959 (UNGA 1959). UNCOPUOS is now the principal multilateral body involved in the development of international space law. In addition to States, a number of international organizations, including both intergovernmental and nongovernmental organizations, have observer status with UNCOPUOS.

The first question that was posed to UNCOPUOS sought a clarification as to the legal categorization of outer space for the purposes of international law. In order to be in a position to do this, a legal definition of what constituted outer space and where it began was required. While many theories have been put forward since the question was first posed, where air space “ends” and outer space “begins” has thus far remained unanswered from an international legal viewpoint.

Notwithstanding the lack of a clear definition of outer space, a number of fundamental legal principles relating to the exploration and use of outer space quickly emerged – in particular the so-called “common interest,” “freedom,” and “non-appropriation” principles. These principles were later incorporated into the terms of the United Nations Space Law Treaties, for example Articles I and II of the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space including the Moon and other Celestial Bodies, with the result that they also constitute binding conventional rules codifying what had already amounted to principles of customary international law. In essence, the international community, including both of the major space-faring States of the time, had accepted that outer space was to be regarded as being similar to a *res communis omnium* (Cassese 2005).

The aforementioned three fundamental rules that underpin the international law of outer space represent a significant departure from the legal rules relating to air space, which is categorized as constituting part of the “territory” of the underlying State. The principal air law treaties reflect the territorial nature of air space.

For example, reaffirming the principle already acknowledged as early as 1919 (ICAN 1919), the 1944 Convention on International Civil Aviation (ICAO 1944) provides that “every State has complete and exclusive sovereignty over the air space above its territory” (ICAO 1944). Even though, a demarcation between air space and outer space has not yet definitively emerged – at least thus far – this has not in practice led to any significant confusion as to “which law” might apply in particular circumstances (Freeland 2010b). However, as the range of activities in outer space becomes ever broader, the issue will become more important in relation not only to the broad principles of international space law but also on a practical level – for example, to the regulation of commercial suborbital space tourism activities, which, at least under current technological constraints, involve paying passengers being taken to an altitude slightly in excess of 100 km above the Earth (Freeland 2010b).

By contrast, Article II of the Outer Space Treaty encompasses the so-called “non-appropriation” principle, which is regarded as one of the most fundamental rules regulating the exploration and use of outer space (Freeland and Jakhu 2010). The provision reads:

Outer space, including the moon and other celestial bodies, is not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.

In essence, Article II confirms that outer space (which includes the Moon and other celestial bodies) is not subject to ownership rights and prohibits *inter alia* any sovereign or territorial claims to outer space. Outer space therefore is not to be regarded as “territorial,” a principle that, by the time the treaty was concluded in 1967, was already well accepted in practice. This was evidenced by the fact that although the USSR had not sought the permission of other States to undertake the Sputnik mission, there were no significant protests that this artificial satellite had infringed on any country’s sovereignty as it circled the Earth. As was observed by Judge Manfred Lachs of the International Court of Justice (Lachs 1969):

[t]he first instruments that men sent into outer space traversed the air space of States and circled above them in outer space, yet the launching States sought no permission, nor did the other States protest. This is how the freedom of movement into outer space, and in it, came to be established and recognised as law within a remarkably short period of time.

By the time that the Outer Space Treaty was finalized, both the United States and the USSR had already been engaged in an extensive range of space activities. However, neither had made a claim to sovereignty over any part of outer space, including celestial bodies, notwithstanding the planting by the Apollo 11 astronauts of an American flag on the surface of the Moon. This is to be compared with the situation in Antarctica, which had seen a series of sovereign claims by several States in the period leading up to the finalization in 1959 of the Antarctic Treaty, 402 U.N. T.S. 71. Article IV of the Antarctic Treaty has the effect of suspending all claims to territorial sovereignty in Antarctica for the duration of that instrument, as well as prohibiting any “new claim, or enlargement of an existing claim.” The Protocol on

Environmental Protection to the Antarctic Treaty, 30 I.L.M. 1455, which came into force in 1998, augments the Antarctic Treaty by protecting Antarctica from commercial mining for a period of 50 years. As a result, although it was of great importance to formalize this principle of non-appropriation of outer space, the drafting process leading to the finalization of Article II of the Outer Space Treaty was relatively uncontroversial, particularly given its early acceptance as a fundamental concept by these two space faring States.

It is no coincidence that the non-appropriation principle is set out immediately following Article I of the Outer Space Treaty, which elaborates on the “common interest” and “freedom” principles and confirms that the exploration and use of outer space is to be undertaken “for the benefit and in the interests of all countries” and freely “by all States without discrimination of any kind, on a basis of equality and in accordance with international law.” In broad terms, the primary intent of Article II was to reinforce these concepts by confirming that principles of territorial sovereignty do not apply to outer space. Not only does this reflect the practice of States from virtually the beginning of the space age but it also helps to protect outer space from the possibility of conflict driven by territorial or colonizing ambitions.

There has, however, been one notable exception in this regard – the Bogota Declaration. In 1976, a number of equatorial States – including Brazil, Colombia, the Congo, Ecuador, Indonesia, Kenya, Uganda, and Zaire – issued the Bogota Declaration, in which they claimed sovereign rights over segments of geostationary synchronous orbit above their respective territories. They asserted their claims principally because of the lack of an accepted delimitation between airspace and outer space. Such assertions were strenuously opposed by other States and have not been successful.

In this regard, the sentiments reflected in Article II of the Outer Space Treaty are fundamental to the regulation of outer space and its exploration and use for peaceful purposes. It is for these reasons that a binding principle of non-appropriation is an essential element of international space law.

Unlike the corresponding provision in United Nations Convention on the Law of the Sea (UNCLOS) (1982) dealing with the high seas, Article II does not expressly limit itself to the purported actions of States; rather, the provision is drafted in more general terms, in that it seeks to prohibit specific actions that constitute a “national appropriation.” One should note, however, that the Chinese version of the Outer Space Treaty differs in this respect from all other versions, in that it prohibits appropriation “through the state by asserting sovereignty, use, occupation or any other means.” In accordance with Article XVII of the Outer Space Treaty, the Chinese version is “equally authentic” with all other versions. However, it has also been noted that the fact that the other four versions (English, Russian, French and Spanish) all concur on the text of the provision is significant, “the more so if they include the languages which were mostly used in negotiations of the Outer Space Treaty” (Kopal 2006). With the obvious exception of the reference to “by claim of sovereignty,” there is no express limitation in Article II *only* to the actions of States. This has, over the years, given rise to frequent debate among commentators as to the

precise scope of the prohibition and, more particularly, the extent (if at all) to which “private property rights” (Harris 2004) may exist in outer space, notwithstanding (or perhaps as a result of) the terms of Article II.

In other aspects, the degree to which international law governs outer space is not entirely clear. The Outer Space Treaty affirms that activities in space are to be carried on “in accordance with international law,” (UNGA 1967, Article III) but the fact that most existing international law at the time was developed for “terrestrial” purposes meant that it was not readily or directly applicable in every respect to this new paradigm of human endeavor. Moreover, the non-sovereignty aspect of outer space meant that any then existent national law (which, in any event, did not at that time specifically address space-related issues) would not *prima facie* apply to this frontier, and would not be the appropriate legal basis upon which to establish the initial framework for regulating the conduct of humankind’s activities in outer space. It was clear, therefore, that, at the dawn of the development of “space law,” specific international binding rules would be required to address the particular characteristics and legal categorization of outer space.

There is now a substantial body of law dealing with many aspects of the use and exploration of outer space, mainly codified in and evidenced by Treaties, United Nations General Assembly resolutions, national legislation, the decisions of national courts, bilateral arrangements, and determinations by Intergovernmental Organizations.

Five important multilateral treaties have been finalized through the auspices of UNCOPUOS (UNGA 1959). These are:

- (i) 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies (UNGA 1967)
- (ii) 1968 Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (UNGA 1968)
- (iii) 1972 Convention on International Liability for Damage Caused by Space Objects (UNGA 1972)
- (iv) 1975 Convention on Registration of Objects Launched into Outer Space (UNGA 1975)
- (v) 1979 Agreement Governing the Activities of States on the Moon and other Celestial Bodies (UNGA 1979)

The United Nations Space Treaties were formulated in an era when only a small number of countries had space-faring capability. The international law of outer space thus, at least partially, reflects the political pressures imposed by the superpowers at that time.

The United Nations General Assembly has also adopted a number of space-related Principles, which include:

- (i) 1963 Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space (UNGA 1963)



- (ii) 1982 Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting (UNGA 1982)
- (iii) 1986 Principles Relating to Remote Sensing of the Earth from Outer Space (UNGA 1986)
- (iv) 1992 Principles Relevant to the Use of Nuclear Power Sources in Outer Space (UNGA 1992)
- (v) 1996 Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries (UNGA 1996)

These sets of principles provide for the application of international law and the promotion of international cooperation and understanding in space activities, the dissemination and exchange of information through transnational direct television broadcasting via satellites and remote satellite observations of Earth, and general standards regulating the safe use of nuclear power sources necessary for the exploration and use of outer space. More recent “guidelines” have also been agreed relating to various other issues, including the problem of space debris (UNCOPUOS 2007).

In the context of the regulation of the exploration and use of outer space, these five sets of principles have therefore largely been considered as constituting “soft law” (Freeland 2012); however, a number of specific provisions may now represent customary international law.

Yet, despite all of these developments, it is clear that the existing legal and regulatory regime has not kept pace with the remarkable technological and commercial progress of space activities since 1957. This represents a major challenge in relation to the ongoing development of effective legal principles, all the more in view of the strategic and military potential of outer space in an era of globalization.

---

## Principles Regulating the “Military” Uses of Outer Space

The Outer Space Treaty provides a number of general principles that are intended to restrict the military uses of outer space, including the requirement that activities in the exploration and use of outer space shall be carried out “in accordance with international law, including the Charter of the United Nations” (UNGA 1967, Article III). One of the primary drivers behind the inclusion of this provision was the concern among many States that outer space would become a new arena for international conflict. Article 2 of the Moon Agreement extends these sentiments by referring to “the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations” (UNGA 1970).

As noted, many of the fundamental principles that formed the basis of the Outer Space Treaty were concluded at a time when the world was in the midst of uncertainty and mistrust, largely as a result of the prevailing geopolitical environment of the Cold War. At the time, there was a genuine fear held by the international

community that outer space would be utilized for military purposes, as well as concern that it could perhaps ultimately become a theatre of war. In December 1958, the United Nations emphasized the need “to avoid the extension of present national rivalries into this new field” (UNGA 1958).

By 1961, the General Assembly had recommended that international law and the United Nations Charter should apply to “outer space and celestial bodies” (UNGA 1961). This was repeated in General Assembly Resolution 1962, which set out a number of important principles that were ultimately incorporated into the Outer Space Treaty (UNGA 1963). The specific reference to the United Nations Charter was considered to be important, given that the maintenance of international peace and security is the underlying principle of the system established under that instrument (UN 1945).

The sentiments underlying the United Nations Charter were strengthened further by the restrictions imposed in relation to nuclear weapons and weapons of mass destruction by Article IV of the Outer Space Treaty, although, as has been well documented by leading commentators, this provision in and of itself does not represent a complete restriction on the placement of weapons in outer space, nor of their use (Schrogl and Neumann 2009). Indeed, there have been, from time to time, proposals put forward to amend Article IV in order to enhance these restrictions, but this has not (yet) eventuated (Bogomolov 1993).

The “peaceful purposes” provision set out in Article IV of the Outer Space Treaty has been the subject of much analytical discussion as to its scope and meaning. While there exists some consensus among space law commentators – but not complete unanimity – that this provision is directed against “nonmilitary” rather than merely “nonaggressive” activities, the reality has been different. As noted, it is undeniable that, in addition to the many commercial, civilian, and scientific uses, outer space has and continues to be used for an expanding array of military activities. Gone are the days where there existed only two superpowers leading the world in space technology and exploration. The modern space age sees a new space race that exists among existing and emerging powers. It has now been established that competitive capabilities in outer space directly correlate to strategic and military capabilities on Earth.

In this context, if one were to adopt a hard-line pragmatic view, the “nonmilitary vs. nonaggressive” debate relating to the peaceful purposes requirement is a redundant argument, even though it represents an extremely important issue of interpretation of the strict principles of international space law. This then assumes that the militarization of space is a given, as much as it may pain international and space lawyers to admit this.

Moreover, Article 51 of the United Nations Charter – which confirms the “inherent right” of self-defense “if an armed attack occurs” – is also applicable to the legal regulation of outer space. Under the principles of public international law, this right remains subject to express legal limitations – the requirements of necessity and proportionality (ICJ 2003). Even where the right of self-defense is lawfully exercised, the State so acting will remain subject to the laws of war. While this is, in theory, uncontroversial, the difficulty is to determine precisely whether (and how)

these fundamental principles can be applied to the unique legal and technological context of outer space.

This is particularly relevant given that the use of satellite technology already represents an integral part of the military strategy and the conduct of many armed conflicts. With space capabilities and technology developing at a rapid pace, any case of armed conflict in the twenty-first century and beyond will continuously involve the utilization of outer space. This is the direction and environment that the current political climate it operates in.

While the weaponization of space flies in the face of the principles of the Outer Space Treaty, it would be naive to ignore the realities of the twenty-first century. It would rather be more pragmatic to understand both what (and how) existing legal principles, including the rules of the laws of war, apply to any military activities involving outer space and to determine what needs to be done to provide, at least from a regulatory perspective, an appropriate framework to protect humankind in the future.

---

## The Laws of War: General Principles

Over time, the international community has gradually agreed upon the principles of the laws of war (also known as international humanitarian law or the *jus in bello*) designed to provide legal constraints applicable to the conduct of armed conflict. It is only relatively recently that these minimum international standards have been developed to regulate *how*, *with what*, and *against whom* wars could be fought. It is interesting to note that “war” as a concept was declared illegal by the 1928 Pact of Paris (Kellogg–Briand 1929). Facing the realities of the modern world, it is evident that armed conflict still continues and has become more complex over time. This is not only due to the rapidly developing technology that has become increasingly integral to the conduct of armed conflict but also to the increasing role of non-State actors in conflict. As such, the scope for cataclysmic destruction and loss of life has increased due to the development of sophisticated weaponry, which includes the use of space technology.

The origins of the “laws and customs of war” were from the customary practices of armies on the battlefield and has since developed as a principal branch of international law (Henckaerts and Doswald-Beck 2005). The application of these customary practices was not uniform, and it therefore became evident that more formalized standards were required. A major step forward in the development of the rules of war, which inter alia limit the method and means of conducting warfare and also provide for classes of protected persons and protected objects, came with the Brussels Conference of 1874 and, more significantly, The Hague Peace Conferences of 1899 and 1907, which gave rise to some important standard-setting treaties that are still applicable today. The 1899 Conference concluded that “[t]he right of belligerents to adopt means of injuring the enemy is not unlimited” (U.K.T.S. 1899).

As time went on, further treaties followed, each specifying in greater detail the limits of what constituted (un)acceptable behavior in the context of armed conflict.

For instance, those provisions of the Hague Conventions that applied the laws of war to restrict the use of poison or poisoned weapons and asphyxiating gases were further extended by the 1925 Geneva Protocol (L.N.T.S. 1929).

The scars of the Second World War demonstrated the inadequacy of the existing rules, especially in respect to the treatment of civilians and noncombatants. The critical four 1949 Geneva Conventions were concluded to address these issues, (UNGA 1929, 1949a, b, c, d) and these were strengthened by the Additional Protocols of 1977 (UNGA 1949a, b, c, d, 1977). There have also been a growing number of other important treaties that have added to the corpus of international humanitarian law and the rules regulating armed conflict, particularly in relation to restrictions on specific weapons and means of warfare. Among these are several treaties that relate to the use of outer space, including those limiting the testing of nuclear and other weapons (UNGA 1963, 1972, 1996, 1998), as well as the 1977 Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD) (UNGA 1977), which was the first instrument that dealt with deliberate destruction of the environment during warfare, although it also applies in time of peace.

International humanitarian law is now a well-developed area of international law, covering many aspects of terrestrial warfare. The obligations that arise under the fundamental principles of international humanitarian law, particularly those contained in The Hague Conventions and the Geneva Conventions and their Additional Protocols, have been reaffirmed by the United Nations Security Council (UNSC 2006). Moreover, the formation of multiple national, regional, and international enforcement mechanisms of justice – culminating in the International Criminal Court, the world’s first permanent court of its kind – clearly indicates that the international community is determined that those senior officials (both military and political) who breach these established standards are to be held to account (Freeland 2006).

While there are many principles that have arisen through the evolution of the *jus in bello*, there are three specific concerns that form the basis of any decision to undertake an act of military engagement. They are the principles of distinction, military objective, and proportionality. Each of these is relevant to a consideration of the applicability of the laws of war to the use of outer space. Many commentators combine issues of distinction and military objective into a broader principle known as “discrimination.” However, by differentiating between these two issues, it emphasizes the need to distinguish between civilians and combatants without reference to sometimes subjective considerations as to what constitutes a military target in the context of military advantage.

## Distinction

Under the principle of distinction, deliberate attacks against civilians and noncombatants are prohibited. Article 48 of Additional Protocol I provides inter alia that “[i]n order to ensure respect for and protection of the civilian population . . . the Parties

to a conflict shall at all times distinguish between the civilian population and combatants” (UNGA 1977). In addition, those engaged in armed conflict must not use weapons that are incapable of distinguishing between combatants and non-combatants. These represent fundamental concepts in the conduct of military activities and illustrate the strong linkages between the scope of international humanitarian law and the development of formal legal principles for the human rights of the individual. In his Dissenting Opinion in *Legality of the Threat or Use of Nuclear Weapons*, Judge Koroma pointed out that “both human rights law and international humanitarian law have as their *raison d’être* the protection of the individual as well as the worth and dignity of the human person, both during peacetime or in an armed conflict” (Koroma 1996).

### **Military Objective**

The principle of military objective asserts that attacks not directed at a legitimate military target are prohibited. The important issue is the need to distinguish between civilian persons or objects and military objectives – comprising the elements of “effective contribution to military action” and “definite military advantage” specified in Article 52 of Additional Protocol I (UNGA 1977). Article 52 of Additional Protocol I provides inter alia that “[i]n so far as objects are concerned, military objectives are limited to those objects which by their nature, location, purpose or use make an effective contribution to military action and whose total or partial destruction, capture or neutralization, in the circumstances ruling at the time, offers a definite military advantage” (UNGA 1977).

### **Proportionality**

The principle of proportionality promulgates that even when attacking a legitimate military objective, the extent of military force used and any injury and damage to civilians and civilian property should not be disproportionate to any expected military advantage. This standard demands an assessment of any potential “collateral damage” in the case of military action. However, in practice, it is often difficult to apply the proportionality principle given that different people and States ascribe differing relative “values” to military advantage *vis-à-vis* civilian injury and damage. One only need recall the Advisory Opinion in the *Legality of the Threat or Use of Nuclear Weapons*, where the International Court of Justice, while noting that the threat or use of a nuclear weapon should comply with the requirements of international law relating to armed conflict, in particular, the principles of international humanitarian law, could not say categorically that the threat or use of nuclear weapons would in every circumstance constitute a violation of international law (ICJ 1996).

## The Relevance of the Laws of War to Outer Space

As noted above, the existing principles of international humanitarian law, as an integral part of international law, are, in theory, applicable to the military use of outer space. There is no specific “territorial” limitation to the laws and customs of war, which apply both to the area where the hostilities actually take place, as well as to other areas affected by those hostilities. If, for example, direct military action takes place in one area, but the effects of that action impact on civilians elsewhere, that represents a relevant consideration in determining whether such action is consistent with, for example, the principle of proportionality. As a result, any military activity that takes place in outer space will *prima facie* be subject to the *jus in bello* in relation not only to that direct action but also as to its effects and consequences elsewhere, including on Earth.

Having reached this conclusion, it is then necessary to determine whether the rules of war are “relevant” to activities in outer space. Looking at past and current events, the answer appears self-evident. During the Gulf War in 1990, the military value of space assets were first utilized for the conduct of warfare. Indeed, “Operation Desert Storm” is regarded as “the first space war” (Maogoto and Freeland 2007). It was recognized that the use of space technology would create an “integrated battle platform” to aid in the implementation of military strategy. Following the attacks of 11 September 2001, the United States Administration embarked on a policy designed to dominate the space dimension of military operations. This necessitates having the ability to protect critical US infrastructure and assets in outer space. The United States’ approach to military advantage has now become heavily reliant upon space capabilities. The latest announcement from the Trump Administration establishing a “Space Force” further indicates the pivot of the United States military towards outer space, an area that it has increasingly designated as the newest “war-fighting domain.”

Further, the reliance on space assets by other leading space-faring nations such as Russia and China illustrates the global space race that is developing in outer space. China has been rapidly consolidating its status as a space power, adding further to the tensions relating to space-related weapons technology. The first Gulf War demonstrated to China’s military leadership the importance of high-tech integrated warfare platforms, and the ability of sophisticated space-based command, control, communications, and intelligence systems to link land, sea, and air forces. While one of the strongest motivations for China’s space program appears to be political prestige and scientific exploration, China’s space efforts will almost certainly contribute to the development of improved military space systems.

While not the leading space-faring power that it once was at the height of the Cold War, Russia still maintains a strong focus on developing its space capabilities and striving for technical dominance in this domain. The European Union has also identified outer space as “a key component for its European Defence and Security Policy” (Hagen and Scheffran 2005). Even for smaller countries such as Australia,

the political landscape of national space policy highlights military and national security concerns (Freeland 2010a).

In this context, several commentators have opined that space warfare is, in fact, inevitable and cannot be avoided (De Angelis 2002). If these assertions turn out to reflect reality, the principles of the laws of war should be applied. However, it is not clear how this will be done in practice and what consequences will follow.

One complicating factor in this analysis is the increasing prevalence of what are referred to as “dual-use” satellites. The concept of a dual-use facility or resource – typically a commercial facility or resource that is also utilized by the military for military purposes – has become a common feature of contemporary technological society. This presents particular difficulties for those conducting armed conflict, since an asset that could *prima facie* be regarded as a legitimate military target on the basis of military objectives (see further below) might also – even at the same time – be operating for civilian/commercial uses. It is sometimes very difficult, or indeed impossible, to “quarantine” what is the civilian/commercial aspect of a facility from the military component. Additionally, military “customers” are now regularly utilizing commercial satellites to undertake military activities. In this respect, the language of the international law instruments relating to outer space has not hampered the increasing utilization of satellite technology for an expanding array of military activities.

One terrestrial example is illustrative of the difficulties of engaging in a straightforward legal analysis of any attack against such a facility. During the 1999 NATO bombing campaign directed towards forcing the Serbian military to leave Kosovo (known as “Operation Allied Force”), one deliberate target was the RTS Serbian TV and Radio Station in Belgrade. NATO missiles destroyed the station on 23 April 1999, with significant – and only civilian – loss of life. The bombing of the TV studio was part of a planned attack aimed at disrupting and degrading the C3 (Command, Control, and Communications) network of the Government of the Former Yugoslavia.

At a press conference on 27 April 1999, NATO officials justified this attack in terms of the dual military and civilian use to which the communication system was routinely put (NATO 2000; Freeland 2002). In essence, NATO stressed the dual-use to which such communications systems were put, emphasizing the fact that “military traffic is . . . routed through the civilian system” (NATO 2000).

This concept is, as noted above, also a common feature of space technology. A combination of factors – the increasing dependence by military and strategic forces within (the major) powers on the use of satellite technology; the inability of Governments to satisfy such demands for reasons associated either with costs or the lack of technological expertise (or both); and the advent of commercial satellite infrastructure and services that are responsive, technologically advanced, available, and appropriate to meet these demands – means that military “customers” are now regularly utilizing commercial satellites to undertake military activities. Given that such an increasingly important group of space assets used for military purposes are these dual-use satellites, one is also drawn to the question of whether, and in what circumstances, such a satellite can (ever) be regarded as a legitimate target of war.

The answer will depend upon a number of fundamental principles of international law. Clearly, the physical destruction of a satellite constitutes a use of force. Apart from a consideration of the principles in the United Nations Space Treaties, one would have to determine whether such an action represents a legitimate (at law) use of force, with the only possible justification being Article 51 of the United Nations Charter.

For example, assume that a combatant regards a dual-use satellite – in this scenario, a GPS or remote sensing satellite – as representing a legitimate military objective in accordance with the principles of distinction and military advantage. Even if this were a correct assessment, the principle of proportionality would also apply. Moreover, one could argue that, implicit in the principle of distinction is the obligation on the parties to a conflict to take “all feasible precautions” to protect civilians from the effects of an attack (Henckaerts and Doswald-Beck 2005). There would also be adverse environmental consequences (including significant space debris) resulting from the destruction of a satellite, and various international environmental law principles would therefore also be applicable in these circumstances.

One can certainly envisage that the deliberate destruction of such a satellite could, even if it does not result in any immediate civilian casualties, have a devastating impact on communities, countries, or even regions of the world. Millions of lives and livelihoods could, potentially, be affected, economies destroyed, and essential services incapacitated. Naturally, some of the consequences of such an attack may be difficult to foresee, but it would, one could argue, be regarded at the least as reckless. However, there is likely to be some uncertainty as to whether and how a “recklessness” test is to be applied in such a situation (Freeland 2002).

Overall, given the unique nature of outer space, the fundamental principles of the laws of war – developed to regulate *terrestrial* warfare and armed conflict – are probably neither sufficiently specific nor entirely appropriate for military action in outer space. Even though every effort should be made to apply the existing principles as directly as possible, the largely unprecedented nature of such an environment means that more specific rules will almost certainly be required, if they are to provide a comprehensive framework to properly protect humanity from the disastrous consequences of outer space becoming another theatre of warfare.

---

## **Regulating the Threat of Space Warfare: Some Recent Initiatives**

There is reluctance among the major powers to address the question of international space law regulation through the use of binding treaty instruments. As such, a voluntary soft law approach has been preferred, such as utilizing “transparency and confidence building measures” (TCBMs). A principal TCBM in the area of space regulation had been the (draft) International Code of Conduct for Outer Space Activities (CoC), which was initially developed as a European initiative but has since become broader in scope (European External Action Service 2014). Discussions in 2015 intended to facilitate agreement on this instrument failed, with the instrument now not seriously referred to in relevant fora.



Space debris, an issue that was addressed in the draft CoC, is increasingly becoming a signification risk to operations in outer space as on-orbit collisions can have catastrophic repercussions and leads to further creation of debris. Related to the issue of space debris is, of course, the issue of maintaining the integrity of space assets, both in terms of adhering to measures on debris control and mitigation as well as remediation. Equally it serves to minimize the possibility that a state would destroy another state's satellite (and in the process almost certainly create additional space debris).

Another approach was that of the Draft Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects (PPWT). Since the early 1980s, there have been a series of United Nations General Assembly (UNGA) Resolutions on the specific issue of preventing an arms race in outer space. Such Resolutions focused on addressing this issue and drew further attention of the international community to the need to respond to various military initiatives taken by major space powers in their use of outer space. Ostensibly responding to these calls, in February 2008, the then Minister of Foreign Affairs of the Russian Federation, Sergey Lavrov, presented a draft document headed "Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects" to the 65 members attending the Plenary Meeting of the United Nations Conference on Disarmament (CD) in Geneva. The PPWT had been developed by Russia and China, two of the major space superpowers in the world.

The formal submission of the PPWT to the CD followed several years of diplomatic discussion, directed towards agreeing the terms of legally binding rules addressing the dangers of an arms race in space. In general terms, the PPWT focused on three primary obligations of States Parties, each of which are specified in Article II: not to place in orbit around the Earth, install on celestial bodies, or station in outer space in any other manner "any objects carrying any kind of weapons"; not to "resort to the threat or use of force against any outer space objects"; and not to encourage another State(s) or Intergovernmental Organization to "participate in activities prohibited" by the PPWT.

In responding to the PPWT, the United States Administration has continually reiterated that it opposes any treaty that seeks "to prohibit or limit access to or use of space," adding that, in any event, such a treaty would be impossible to enforce. Indeed, verification measures in relation to the obligations of State Parties under the PPWT would undoubtedly prove to be difficult and complex – though perhaps not impossible – to implement. Instead, the United States has indicated that it prefers "discussions aimed at promoting transparency and confidence building measures."

Overall however, and despite its shortcomings, the PPWT has raised issues of crucial importance to the future use and exploration of outer space, indeed to the very nature of space activities. It was therefore unfortunate that the document was so quickly rejected out of hand by the United States. Indeed, in February 2008, barely a week after Russia and China submitted the PPWT to the CD, the United States fired an SM-3 missile from USS Lake Erie that destroyed a failed satellite approximately 150 km above the Pacific Ocean. Although the United States argued that this action

was necessary to prevent the fuel tank of the satellite – containing hydrazine – from breaking up and polluting the atmosphere, others have suggested that this was simply a “test” by the United States of its anti-satellite capability.

Yet, despite these setbacks, the formal submission of the PPWT by two of the world’s space superpowers has had the effect of generating further momentum in relation to other initiatives to address the impending perils associated with the possible weaponization of space, for instance, the draft CoC.

While there are obvious benefits in developing greater trust between the space powers in issues relating to space security, the danger of the aforementioned TCBMs is that they are nonbinding TCBM. For all practical purposes, they considered as the “end game” on this issue, so that the formalization of binding obligations may *never* emerge.

At its core, the draft CoC provisions, for example, are merely guidelines or recommendations that do not have the force of law, unless they are to be regarded as reflecting rules of customary international law, itself a very difficult assertion to substantiate in the absence of, say, a ruling by the International Court of Justice. This approach appears inadequate to meet the complex risks associated with the continued development of space-related weapons.

---

## **Conclusion: Perspectives on the Way Forward**

The above brief discussion gives rise to several conclusions and reflections: first, present indications suggest that there is an increasing likelihood that outer space will not only be used to facilitate armed conflict (as it already is) but will ultimately become a theatre of war. The tendency of the major superpowers to unequivocally rely on space technology has spurred a space weapons race, despite the efforts of the international community. Even though the United States may currently claim space superiority, leading nations such as China and Russia closely follow behind and have access to equally sophisticated (and potentially devastating) space weapons technology.

Secondly, the development of such technology and the increasing range of military uses of outer space heighten the dangers of a space war. The proliferation of crucial military space assets means that, from a military and strategic viewpoint, the disabling or destruction of satellites used by another country may be perceived as giving rise to very significant advantages. The fact that it has not happened in the past is no reason to assume that we will never see a space conflict.

Thirdly, all countries in the world are highly dependent on space technology to maintain and improve their livelihood and standard of living. The nonmilitary uses of space have become vital aspects of any community’s survival. At the same time, however, many of the satellites providing these commercial and civilian services are dual-use, in that they are also utilized for military and strategic purposes. This raises difficult questions about the “status” of such assets under the rules of war – particularly as to whether they may, under certain circumstances, be regarded as legitimate military objectives.

Fourthly, the Outer Space Treaty, which also reflects customary international law, specifies that the rules of international law apply to the use and exploration of outer space. These include not only the *jus ad bellum* principles regulating the use of force but also the principles of the laws of war. Respect for these rules is absolutely vital for the safety and security of humankind, as well as the interests of future generations. However, with the exception of those treaties that seek to ban the use and testing of certain types of weapons, as discussed there are many uncertainties that arise when one seeks to apply, in particular, the laws of war to a space conflict. The consequences of a space war are potentially so great and unknown that one cannot be sure as to exactly how these existing rules are to apply.

Fifthly, if we are to avoid “gray areas” in the law, it is therefore necessary to develop specific and clear rules and standards that reduce the weaponization of outer space, as well as any form of conflict in the region of outer space and against space assets. The Outer Space Treaty, as well as the other United Nations Space Treaties, do not currently provide stringent rules or incentives to prevent an arms race in outer space, let alone a conflict involving (and perhaps “in”) space. This may, therefore, require additional specific legal regulation of outer space that is directly applicable to armed conflict involving the use of space technology. The position is, of course, further complicated by the applicability of the right of self-defense, a right that States will never abandon.

As part of these new rules, clear definitions must be developed for concepts such as “space weapons,” “peaceful purposes,” and “military uses.” Moreover, the fundamental issue of “where space begins” should be definitively resolved, so as to counter any arguments that outer space is, in fact, an area akin to the territory of a State for the purposes of national security.

Sixthly, at the same time, careful consideration must be given to the application of the principles of the laws of war to this new paradigm of potential conflict. While, of course, there already exist very well established fundamental rules regulating terrestrial warfare, it is not clear whether these are entirely sufficient to protect humanity from the consequences of any future “space wars.” Ultimately, the legal regulation of outer space is not likely to take the form of binding treaty obligations which supplement the existing laws of war (as they may apply to such activities) in the short-medium term, but rather will be on a voluntary nonbinding basis. This illustrates the sensitivities related to further regulating outer space activities that relate to issues of national security interests, particularly those of the major space powers.

It seems that a “softly, softly” approach involving the development of TCBMs is the preferred strategy, particularly of the United States, but this brings with it much more uncertainty, a lack of formal enforcement capability and enforcement mechanisms, and the possibility of undue flexibility of approach by the main global players. It is imperative on all stakeholders to find a path forward, in order to meet the challenges of the twenty-first century. The existing international regulatory framework, while important, cannot alone stand up to the unknowns that military-related space technology imposes upon us. It is critical that an appropriate and acceptable regulatory regime is found; however, the mechanism and conformity that this might take still remains unclear, particularly considering the distinct complexities that outer space presents.

## References

- Bogomolov V (1993) Prevention of an arms race in outer space: the deliberations in the Conference on Disarmament in 1993. *J Space Law* 21(2):141
- Cassese A (2005) *International law*, 2nd edn. Oxford University Press, Oxford/New York, p 95
- Comprehensive Nuclear Test-Ban Treaty (not yet in force), 1998, United Nations, Dept. for Disarmament Affairs and Dept. of Public Information
- Convention on Civil Aviation (“Chicago Convention”), 7 December 1944, International Civil Aviation Organization (ICAO), 15 U.N.T.S. 295 (1944)
- Convention on the Law of the Sea (UNCLOS), 1982, Article 137(1), United Nations Division for Ocean Affairs and the Law of the Sea, United Nations Treaty Series
- Convention on the Prohibition of Military or Any Other Hostile Use of Environmental Modification Techniques (ENMOD), 1977, United Nations, 16 I.L.M. 88
- Convention on the Prohibition of the Development, Production and Stockpiling of Bacteriological (Biological) and Toxin Weapons and on their Destruction, 1972, United Nations, 1015 U.N.T.S. 163
- Convention on the Regulation of Aerial Navigation (“Paris Convention”), 1919, International Commission for Air Navigation (ICAN), 11 L.N.T.S. 173
- De Angelis IM (2002) Legal and political implications of offensive actions from and against the space segment. *Proc Colloq Law Outer Space* 45:197
- Declaration of the first meeting of equatorial countries or ‘Bogota Declaration’, 1976, Heads of Delegations, Japan Aerospace Exploration Agency
- Draft International Code of Conduct for Outer Space Activities, 2014, European External Action Service. [http://www.eeas.europa.eu/non-proliferation-and-disarmament/pdf/space\\_code\\_conduct\\_draft\\_vers\\_31-march-2014\\_en.pdf](http://www.eeas.europa.eu/non-proliferation-and-disarmament/pdf/space_code_conduct_draft_vers_31-march-2014_en.pdf). Accessed 18 Feb 2019
- Final Report to the Prosecutor by the Committee Established to Review the NATO Bombing Campaign Against the Federal Republic of Yugoslavia, 2000, paragraph 72 (2000) 39 I.L.M. 1257 (NATO Report)
- Freeland S (2002) The bombing of Kosovo and the Milosevic Trial: reflections on some legal issues. *Aust Int Law J* 150:165–168
- Freeland S (2006) How open should the door be?: Declarations by non-states parties under Article 12(3) of the Rome Statute of the International Criminal Court. *Nord J Int Law* 75(2):211
- Freeland S (2010a) Sensing a change? The re-launch of Australia’s space policy and some possible legal implications. *J Space Law* 36(2):381
- Freeland S (2010b) Fly me to the Moon: How will international law cope with commercial space tourism? *Melb J Int Law* 11(1):90
- Freeland S (2012) The role of ‘soft law’ in public international law and its relevance to the international legal regulation of outer space. In: Marboe I (ed) *Soft law in outer space: the function of non-binding norms in international space law*, vol 9, Bohlau Publishing (Austria)
- Freeland S, Jakhu R (2010) Article II. In: Hobe S, Schmidt-Tedd B, S. Hobe S, Schmidt-T B, Schrogl K.-U (eds) *Cologne Commentary on Space Law*, vol. 1. Outer Space Treaty, Carl Heymanns Verlag, Köln
- General Treaty for the Renunciation of War (“Kellogg–Briand Pact”), U.K.T.S., 1929, Article I, p 29
- Geneva Convention for the Amelioration of the Condition of the Wounded, Sick and Shipwrecked Members of Armed Forces at Sea, 1949, United Nations, 75 U.N.T.S. 85 (UNGA 1949a)
- Geneva Convention for the Amelioration of the Condition of the Wounded and Sick in Armed Forces in the Field, 1949, United Nations, 75 U.N.T.S. 31 (UNGA 1949b)
- Geneva Convention Relative to the Protection of Civilian Persons in Time of War, 1949, United Nations, 75 U.N.T.S. 287 (UNGA 1949c)
- Geneva Convention Relative to the Treatment of Prisoners of War, 1929, United Nations, 75 U.N.T.S. 135 (UNGA 1949d)
- Hagen R, Scheffran J (2005) International space law and space security – expectations and criteria for a sustainable and peaceful use of outer space. In: Benkö M, Schrogl K.-U (eds) *Space law:*

- current problems and perspectives for future regulation, vol 273, Eleven International Pub. (Utrecht, The Netherlands), pp 281–282
- Hague Convention II, 1899, [1907] Supp 1 American Journal of International Law 129, United Nations
- Harris DJ (2004) Cases and materials on international law, 6th edn. Sweet & Maxwell, London, p 252
- Henckaerts J-M, Doswald-Beck L (2005) Customary international humanitarian law – Cambridge University Press (Cambridge), vol 1: Rules, xxv, p 70
- Kopal V (2006) Comments on the issue of “Adequacy of the current legal and regulatory framework relating to the extraction and appropriation of natural resources of the Moon”. In: Policy and law relating to outer space resources: examples of the Moon, Mars, and other celestial bodies, (28–30 June 2006) workshop proceedings. McGill Institute of Air & Space Law, Montreal, pp 227–230
- Legality of the Threat or Use of Nuclear Weapons, 1996, p 577, 1 ICJ Rep. 245, Judge Koroma Dissenting Opinion
- Lyall F, Larsen PB (2009) Space law: a treatise. Ashgate, Farnham, pp 3–9
- Maogoto J, Freeland S (2007) Space weaponization and the United Nations Charter: a thick legal fog or a receding mist? *Int Lawyer* 41(4):1091–1107
- Moon Agreement, 1979, United Nations Treaty Collection. 1363 U.N.T.S. 3
- North Sea Continental Shelf Cases (Federal Republic of Germany v. Denmark and Federal Republic of Germany v. The Netherlands), Judgment, 1969 p 230, I.C.J. 3, Dissenting Opinion of Judge Lachs
- Outer Space Treaty, 1967, United Nations Treaty Collection. 610 U.N.T.S. 205
- Protocol for the Prohibition of the Use in War of Asphyxiating, Poisonous or Other Gases, and of Bacteriological Methods of Warfare, 1929, United Nations, xciv L.N.T.S. 65–74
- Protocol I Additional to the Geneva Conventions of August 12, 1949, and relating to the Protection of Victims of International Armed Conflicts, (Additional Protocol I), 1977, United Nations, 16 I. L.M. 1391
- Protocol II Additional to the Geneva Conventions of 12 August 1949 and relating to the Protection of Victims of Non-International Armed Conflicts, (Additional Protocol II), 1977, United Nations, 16 I.L.M. 1442
- Resolution 26/25, United Nations General Assembly, (XXV), on the Declaration on Principles of International Law concerning Friendly Relations and Co-operation among States in accordance with the Charter of the United Nations (1970)
- Resolution 1348, United Nations General Assembly, (XIII) on Questions on the Peaceful Uses of Outer Space, preambular paragraph 3, (1958)
- Resolution 1472, United Nations General Assembly, (XIV), on International co-operation in the peaceful uses of outer space, (1959)
- Resolution 1674, United Nations Security Council, on the Protection of civilians in armed conflict, paragraph 6, (2006)
- Resolution 1721, United Nations General Assembly, (XVI), on International co-operation in the peaceful uses of outer space, paragraph 1(a), (1961)
- Resolution 1962, United Nations General Assembly, (XVIII), on the Declaration of Legal Principles Governing the Activities of States in the Exploration and Uses of Outer Space, paragraph 4 (1963), United Nations
- Resolution No 37/92, United Nations General Assembly, on the Principles Governing the Use by States of Artificial Earth Satellites for International Direct Television Broadcasting, (1982)
- Resolution No 41/65, United Nations General Assembly, on the Principles relating to Remote Sensing of the Earth from Outer Space, (1986)
- Resolution No 47/68, United Nations General Assembly, on the Principles relevant to the Use of Nuclear Power Sources in Outer Space (1992)

- Resolution No 51/122, United Nations General Assembly, on the Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries (1996)
- Ricks T (2001) Space is playing field for newest war game; air force exercise shows shift in focus. *The Washington Post*, p A1
- Schrogl K-U, Neumann J (2009) Article IV. In: Hobe S, Schmidt-T B, Schrogl K.-U. (eds), *Cologne Commentary on Space Law, Volume I: Outer Space Treaty*, Carl Heymanns Verlag, Köln
- The Caroline Case, ICJ Rep. p 161. (2003). 29 B.F.S.P. 1137–1138; 30 B.F.S.P. 195–196
- Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space and Under Water, 1963, United Nations, 480 U.N.T.S. 43
- Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other Celestial Bodies, 1967, United Nations General Assembly
- UNCOPUOS (2007) Report of the Scientific and Technical Subcommittee on its forty-fourth session. A/AC.105/890, Annex 4, 42. [http://www.oosa.unvienna.org/pdf/reports/ac105/AC105\\_890E.pdf](http://www.oosa.unvienna.org/pdf/reports/ac105/AC105_890E.pdf). Accessed 18 Feb 2019
- United Nations, Charter of the United Nations, 24 October 1945, 1 U.N.T.S. XVI
- United Nations Treaty Collection. 672 U.N.T.S. 119 (1968)
- United Nations Treaty Collection. 961 U.N.T.S. 187 (1972)
- United Nations General Assembly, Convention on Regulation of Objects Launched into Outer Space, United Nations Treaty Collection. 1023 U.N.T.S. 15 (1975)

## Further Reading

- See Lyall F, Larsen PB (2009) *Space law: a treatise*. Ashgate, Farnham, pp 3–9 for a summary of the main academic theories relating to ‘space law’ in the period prior to the launch of Sputnik I
- See United Nations General Assembly Resolution 1472 (XIV) on International Cooperation in the Peaceful Uses of Outer Space (12 December 1959). UNCOPUOS currently has 87 Members, which, according to its website, means that it is ‘one of the largest Committees in the United Nations.’ For more see <http://www.unoosa.org/oosa/en/members/index.html>. Last accessed 18 Feb 2019



# Arms Control and Space Security

# 6

Stacey Henderson

## Contents

Introduction .....	96
Outer Space Treaty .....	96
Moon Agreement .....	98
Arms Control in Outer Space: Historic and Current Efforts .....	99
Partial Test Ban Treaty .....	99
Anti-Ballistic Missile Treaty .....	99
SALT II .....	100
United Nations General Assembly .....	100
Draft Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects .....	102
International Code of Conduct for Outer Space .....	106
Domestic Arms Control for Outer Space .....	107
Conclusions .....	107
References .....	109

## Abstract

With the increasing reliance on space assets for civilian, commercial, and military purposes, there is a need to safeguard their full operability and enhance their security. The uncontrolled use of weapons in outer space has the potential to increase space debris, destroy critical space assets and impair their ongoing functionality, and negatively impact space security. The current international law regime applicable to outer space does not prohibit the placement or use of all weapons in outer space, prohibiting only nuclear weapons and weapons of mass destruction, and is not currently capable of preventing a conventional arms race in outer space.

---

S. Henderson (✉)

Adelaide Law School, The University of Adelaide, Adelaide, SA, Australia

e-mail: [stacey.henderson@adelaide.edu.au](mailto:stacey.henderson@adelaide.edu.au)

## Introduction

At the commencement of the space age, activities in outer space were dominated by two space powers: the United States of America (USA) and the Union of Soviet Socialist Republics (USSR). Today, there are many states, an intergovernmental organization (the European Union), and private actors active in the use and exploration of outer space. As the number of space actors has grown, so too has the reliance on space assets, which are now a critical part of everyday life. The increased dependence on space assets brings with it an increased vulnerability and the need to ensure their security. The continuing growth in the number of space actors and space activities suggests that debates over the placement and use of weapons in outer space will only increase in the future (López 2012).

Arms control has long been discussed between states in the context of space security. Indeed, “the research, development, and testing of aggressive space weapons can be traced back to the 1950s” (Su 2017). Prior to the negotiations on the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (Outer Space Treaty), the USA and the USSR had agreed “not to station in outer space any objects carrying nuclear weapons or other kinds of weapons of mass destruction” (General Assembly Resolution 1884, 1963). Yet the current international legal regime governing outer space does not prohibit all weapons in outer space, prohibiting only nuclear weapons and other weapons of mass destruction. This chapter outlines the international law applicable to arms control in outer space and examines historic and recent efforts to limit the placement and use of weapons in outer space and to prevent an arms race in outer space.

---

## Outer Space Treaty

The Outer Space Treaty is the fundamental international law treaty regulating activities in outer space. All space-faring states are party to the Outer Space Treaty; the Outer Space Treaty has 109 States Parties, with a further 23 states having signed the treaty, but not yet ratified it (as at 19 December 2019).

The Outer Space Treaty is the only one of the four main international space law treaties to specifically address arms control; the Rescue and Return Agreement (1968 *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space*), the Liability Convention (1972 *Convention on International Liability for Damage Caused by Space Objects*), and the Registration Convention (1976 *Convention on Registration of Objects Launched into Outer Space*) are all silent on this issue.

Article IV of the Outer Space Treaty directly addresses the issue of weapons in outer space. Article IV provides:

States Parties to the Treaty undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner.



The Moon and other celestial bodies shall be used by all States Parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manoeuvres on celestial bodies shall be forbidden. The use of military personnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful exploration of the Moon and other celestial bodies shall also not be prohibited.

However, Article IV contains ambiguities, “partly due to the lack of clear terminological definitions, and partly due to subsequent technical developments” (Su 2017).

What would amount to “placement” in outer space is not defined or clarified in the Outer Space Treaty. Some are of the view that a full rotation in orbit is not required in order to amount to placement in orbit (Hobe et al. 2010), whereas others take the view that nuclear armed “pop-up” anti-satellite (ASAT) interceptors that ascend directly to their targets without entering into orbit are not placed into orbit and therefore do not fall within the Article IV prohibition (Bhat and Mohan 2009).

The term “peaceful purposes” is also not defined in the Outer Space Treaty. During negotiations for the Outer Space Treaty, it became clear that neither the USA nor the USSR wanted the Treaty to include a definition of peaceful purposes that might have imposed limitations on their future uses of outer space (Sullivan 1990). As such, the term was left undefined. There are ongoing debates about whether “exclusively for peaceful purposes” means that celestial bodies are to be completely nonmilitarized in the sense that they cannot be used for any military activities, or whether peaceful purposes means that they may be used for non-aggressive military activities (Su 2010). The latter view is more consistent with the terms of the Outer Space Treaty, given that paragraph 2 of Article IV details prohibited and permissible military activities and uses of celestial bodies. If all military activities were prohibited in outer space, there would be no need for paragraph 2 of Article IV.

The Outer Space Treaty prohibits the placement of nuclear weapons and other weapons of mass destruction (generally accepted as including chemical and biological weapons) in outer space or on celestial bodies. It “does not explicitly restrict (and so allows) other military-related activities in outer space, such as the deployment of military satellites and conventional weapons in outer space” (Tronchetti and Hao 2015). The Outer Space Treaty does not prohibit “the deployment of offensive devices in orbit,” provided they are not nuclear or other weapons of mass destruction, nor does it prohibit “the development, storage, and testing of ground-based ASAT devices” (Tronchetti and Hao 2015). The Outer Space Treaty is silent on the use of Earth-based weapons against space objects. It is also unclear whether nuclear devices used to deflect near-Earth objects threatening the Earth should be characterized as weapons and fall within the Article IV prohibition (Su 2017). The ease with which nuclear devices for near-Earth object diversion could be re-purposed for use as nuclear weapons, and the consequential risks of such re-purposing, suggests that they should be covered by the prohibition.

Article IV, paragraph 2, of the Outer Space Treaty imposes restrictions on the military use of celestial bodies and, in the context of arms control, prohibits the testing of any type of weapon on celestial bodies. However, the prohibition on

weapons testing does not extend to outer void space and is limited to a prohibition on weapons testing on celestial bodies.

Article IX of the Outer Space Treaty obliges States Parties to “conduct all their activities in outer space. . .with due regard to the corresponding interests of all other States Parties to the Treaty.” This Article may have incidental application to the testing of Earth-based ASAT weapons, as it imposes obligations on States Parties to avoid harmful contamination, harmful interference, and to undertake appropriate international consultations (Su 2017). However, the standard for avoiding harmful contamination and what is required under the obligation to undertake international consultations are both highly subjective, and Article IX has not been invoked by States in practice when ASAT weapons have been tested, even in situations where large amount of debris were created (Su 2017). Based on subsequent state practice, Article IX must therefore be interpreted as not prohibiting or restricting the testing of Earth-based ASAT weapons.

The Outer Space Treaty regulates space activities and sets the foundation for international space law. The Outer Space Treaty prohibits States Parties from deploying or using nuclear weapons or other weapons of mass destruction in outer space. Additionally, the Outer Space Treaty prohibits States Parties from conducting weapons tests of any kind of weapon on celestial bodies. However, the Outer Space Treaty does not prohibit States Parties from deploying or using conventional weapons in outer space, nor does it prohibit the use of Earth-based weapons against space objects. Additionally, the verification mechanisms in the Outer Space Treaty are very weak, being limited to the opportunity to observe the flight of space objects (Article X, Outer Space Treaty) and a reciprocal right of visitation (Article XII, Outer Space Treaty), falling far short of the verification mechanisms in most arms control agreements.

---

## Moon Agreement

The Moon Agreement (1984 *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies*) mirrors the provisions of the Outer Space Treaty in relation to arms control and is similarly silent in relation to conventional weapons. The Moon Agreement has only 18 States Parties (as at 19 December 2019): Armenia, Australia, Austria, Belgium, Chile, Kazakhstan, Kuwait, Lebanon, Mexico, Morocco, the Netherlands, Pakistan, Peru, Philippines, Saudi Arabia, Turkey, Uruguay, and Venezuela. A further four states – France, Guatemala, India, and Romania – have signed, but not ratified, the Moon Agreement. The Moon Agreement remains unratified by major space-faring states, such as China, Russia, and the USA.

Article 3, paragraph 3 of the Moon Agreement provides:

States Parties shall not place in orbit around or other trajectory to or around the Moon objects carrying nuclear weapons or any other kinds of weapons of mass destruction or place or use such weapons on or in the Moon.

Further, Article 3, paragraph 4 of the Moon Agreement prohibits the “establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military manoeuvres on the Moon.” The Moon Agreement does not impose any additional obligations in relation to arms control on its States Parties beyond those specified in the Outer Space Treaty.

---

## Arms Control in Outer Space: Historic and Current Efforts

### Partial Test Ban Treaty

The 1963 Treaty Banning Nuclear Weapon Tests in the Atmosphere, in Outer Space, and under Water (Partial Test Ban Treaty) entered into force on 10 October 1963. It is one of the most widely accepted international arms control treaties, with 125 States Parties as at 19 December 2019. After signing the Partial Test Ban Treaty, the then two space faring states, the USA and the USSR, reaffirmed “that they did not intend to station any objects carrying WMDs [weapons of mass destruction] in outer space” (Su 2013).

Article I of the Partial Test Ban Treaty provides that

Each of the Parties to this Treaty undertakes to prohibit, to prevent, and not to carry out any nuclear weapon test explosion, or any other nuclear explosion, at any place under its jurisdiction or control:

- (a) in the atmosphere; beyond its limits, including outer space; or under water, including territorial waters or high seas

The Partial Test Ban Treaty is limited to a prohibition of nuclear explosions in outer space, including nuclear weapon test explosions. It does not contain any restrictions on conventional arms in outer space.

### Anti-Ballistic Missile Treaty

The 1972 Anti-Ballistic Missile Treaty (*Treaty between the United States of America and the Union of Soviet Socialist Republics on the limitation of anti-ballistic missile systems*) was a bilateral agreement negotiated between the USA and the USSR as part of the Strategic Arms Limitation Talks (SALT I). The Treaty expressly prohibited the development, testing, and deployment of sea-based, air-based, space-based, and mobile land-based anti-ballistic missile systems (Article V, ABM Treaty). To provide assurance of compliance with the Treaty’s provisions, each Party was to use national technical means of verification, such as satellites, and was not to use deliberate concealment measures or interfere with such verification (Article XII, ABM Treaty). The USA withdrew from the Anti-Ballistic Missile Treaty in June 2002, bringing the treaty to an end.

## SALT II

The 1979 Strategic Arms Limitation Talks II Treaty (SALT II) prohibited “systems for placing into Earth orbit nuclear weapons or any other kind of weapons of mass destruction, including fractional orbital missiles” (Larsen 2017). The Treaty also restricted the USA and the USSR from developing more than one new type of intercontinental ballistic missile each, enforcing that limitation by allowing each party to conduct flight testing of only one new such weapon (Koplow 2018). Verification of the SALTII Treaty obligations was again by national technical means of verification, including reconnaissance satellites. The SALT II Treaty expired on 31 December 1985.

## United Nations General Assembly

### Prevention of an Arms Race in Outer Space

Since 1981, the General Assembly has adopted annual resolutions on the Prevention of an Arms Race in Outer Space (PAROS). The 1988 resolution reaffirmed “that general and complete disarmament under effective international control warrants that outer space shall be used exclusively for peaceful purposes and that it shall not become an arena for an arms race” and called for complete disarmament and effective verification measures (A/RES/43/70, 1988). The resolution passed with a vote of 154 to 1, with only the USA opposing the resolution, which it has repeatedly done on an annual basis.

The 2019 resolution “Further practical measures for the prevention of an arms race in outer space” echoed previous PAROS resolutions and was passed with a vote of 124 in favor to 41 against, with 10 abstentions:

*Recognizing* the catastrophic consequences of the weaponization of outer space or any military conflicts in outer space and that the prevention of an arms race in outer space would avert a grave danger for international peace and security,

...

*Recognizing* that, while the existing international treaties related to outer space and the legal regime provided for therein play a positive role in regulating outer space activities, they are unable to fully prevent the placement of weapons in outer space and therefore avert an arms race there, and that there is a need to consolidate and reinforce this regime, *Expressing serious concern* over the plans declared by certain States that include the placement of weapons, in particular strike combat systems, in outer space,

...

6. *Urges* the international community to continue its efforts aimed at preventing an arms race, including the placement of weapons, in outer space, with a view to maintaining international peace and strengthening global security. (UN Doc A/C.1/74/L.58/Rev.1, 2019)

The PAROS resolutions “typically recognize that the legal regime applicable to outer space is insufficient to guarantee the prevention of an arms race in outer space and there is an urgent need to consolidate and reinforce it, since prevention of an arms race in outer space would avert a grave danger for international peace and

security” (Su 2013). Although recognizing the gaps in the existing international space law regime, and the inability of the current treaty regime to prevent an arms race in outer space, the annual PAROS resolutions do not attempt to establish any normative obligations in relation to arms control and space security. The voting pattern on the PAROS resolutions has significantly changed over the years, indicating that states are now markedly less committed to this ideal than in the past.

### **No First Placement of Weapons in Outer Space**

In October 2004, Russia announced a policy of “no first deployment of weapons in outer space” at the First Committee of the United Nations General Assembly, calling on all other space-faring and space-using states to join them in this pledge (Su 2017). The initiative was supported by other Member States of the Collective Security Treaty Organisation (Armenia, Belarus, Kazakhstan, Kyrgyzstan, and Tajikistan), Brazil, Indonesia, Sri Lanka, Argentina, and Cuba. These states have declared that they “will not in any way be the first to place weapons of any kind in Outer Space, that they will make all possible efforts to prevent Outer Space from becoming an arena for military confrontation and to ensure security in Outer Space activities” (Su 2017).

In 2014, Russia submitted a draft resolution on no first placement of weapons in outer space to the First Committee of the 69th session of the United Nations General Assembly (A/C.1/69/L.14, 2014a). The resolution was adopted by the General Assembly on 2 December 2014 by a vote of 126 in favor and 4 against (Georgia, Israel, Ukraine, and the USA), with 46 abstentions. The US Permanent Representative to the Conference on Disarmament stated that the resolution “does not adequately define space weapons, leaving the nonbinding resolution difficult to enforce, or for compliance with the agreed-upon measures to be verified” (Chow 2018). In explaining its vote, the USA stated that “Russia’s military actions do not match their diplomatic rhetoric,” observed that any space “object with maneuvering capabilities can in theory be used for offensive purposes,” and noted that the lack of a “common understanding of what we mean by a space weapon [in the resolution]. . . would increase mistrust or misunderstanding with regard to the activities and intentions of States” (Plath 2018).

The “No First Placement of Weapons in Outer Space” resolution (GA Res 69/32, 2014b) “encourages all States, especially space-faring nations, to consider the possibility of upholding as appropriate a political commitment not to be the first to place weapons in outer space” (para 5). The resolution relates only to deployment of weapons in outer space and does not restrict research or development of such weapons. Further, the commitment on pledging states is conditional – merely not to be the first to place weapons in outer space; the deployment of weapons in outer space by any other entity, another state or private actor, would free the pledging states from their commitment not to place weapons in outer space. Since the adoption of the No First Placement of Weapons in Outer Space resolution, 22 States have made such a commitment (as at 31 October 2019): Argentina, Armenia, Belarus, Bolivia, Brazil, Cambodia, Cuba, Ecuador, Guatemala, Indonesia, Kazakhstan, Kyrgyzstan, Nicaragua, Pakistan, Russia, Sri Lanka, Suriname, Tajikistan, Uruguay, Uzbekistan, Venezuela, and Vietnam (UN Doc A/C.1/74/L.58/Rev.1, 2019).

The no first placement of weapons in outer space has remained an annual agenda item at the General Assembly since 2014. The most recent resolution in 2019 was passed with a vote of 123 in favor to 14 against, with 40 abstentions. While not imposing any normative obligations on states, these resolutions encourage states to make the political commitment not to be the first to place weapons of any kind in outer space.

---

## **Draft Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects**

The Draft Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force Against Outer Space Objects (PPWT) is a proposed arms control treaty that would impose new definitions, terms, conditions, and obligations on States Parties and fill the gaps in the Outer Space Treaty in relation to arms control. The initial draft PPWT was submitted to the Conference on Disarmament by Russia and China in 2008 (CD/1839, 2008). The draft treaty drew upon a 2002 working paper that had been jointly submitted to the Conference on Disarmament by Russia, China, Indonesia, Belarus, Vietnam, Zimbabwe, and Syria (Su 2010), which confirmed the preference of those states to a hard law approach to the prevention of the weaponization of outer space (Tronchetti and Hao 2015). China has affirmed that it “opposes any weaponization of outer space and any arms race in outer space. . . [and] believes that the best way for the international community to prevent any weaponization of or arms race in outer space is to negotiate and conclude a relevant international legally-binding instrument” (Shimabukuro 2014).

The 2008 initial draft PPWT contains a preamble and 14 Articles. The preamble specifically highlights “the risk that the placement of weapons and an arms race in space pose to the security of space objects as well as to international peace and security as a whole” (Tronchetti and Hao 2015). The draft treaty provides a definition for a weapon in outer space, which is defined as

Any device placed in outer space, based on any physical principle, which has been specially produced or converted to destroy, damage or disrupt the normal functioning of objects in outer space, on the Earth or in the Earth’s atmosphere, or to eliminate a population or components of the biosphere which are important to human existence or inflict damage on them. (Article I(c), CD/1839)

A weapon is considered to be “placed in outer space” if “it orbits the Earth at least once, or follows a section of such an orbit before leaving this orbit, or is permanently located somewhere in outer space” (Article I(d), CD/1839). The draft treaty provides a comprehensive ban on any hostile action against objects in space, defining the use of force and threat of force broadly as

any hostile actions against outer space objects including, inter alia, actions aimed at destroying them, damaging them, temporarily or permanently disrupting their normal

functioning or deliberately changing their orbit parameters, or the threat of such actions. (Article I(e), CD/1839)

The core provision of the 2008 draft PPWT is contained in Article II, which sets out a series of prohibitions:

The States Parties undertake not to place in orbit around the Earth any objects carrying any kinds of weapons, not to install such weapons on celestial bodies and not to place such weapons in outer space in any other manner; not to resort to the threat or use of force against outer space objects; and not to assist or induce other States, groups of States or international organizations to participate in activities prohibited by this Treaty. (Article II, CD/1839)

Article II must be read in conjunction with Articles IV and V, which confirm that nothing in the draft PPWT should be seen as interfering with the right to self-defense or the right to peacefully explore and use outer space. Finally, States Parties are encouraged to implement transparency and confidence building measures (Article VI, CD/1839), although the draft treaty does not establish or recommend any such measures, leaving that to subsequent agreement.

While it was “praised for taking up the challenge of increasing the security of space assets by legal means,” the initial draft PPWT received criticism “for not addressing the most serious threats to space objects, strategically favoring the interests of its co-sponsors and lacking a reliable means of verification” (Tronchetti and Hao 2015). Criticisms leveled against the draft PPWT included its failure to specifically ban the development and testing of Earth-based ASATs (Jaramillo 2009), as well as the overly restrictive definition of “weapon in space” and failure to address “the possible utilization of dual-use satellites and ballistic missiles as means to damage or destroy active space objects” (Tronchetti and Hao 2015). There was also criticism of the broad definition of “use of force” and “threat of force” and the inclusion of a definition of “outer space,” which specified 100 km altitude demarcation; no international agreement on where outer space begins has ever been reached and the delimitation between airspace and outer space has been one of the most controversial topics since the beginning of the space age. The USA staunchly opposed the 2008 draft PPWT and indeed remains opposed to the development of arms control agreements or other restrictions that would restrict its ability to conduct research, development, testing, operations or other activities, or to operate freely in outer space (Jaramillo 2009).

In June 2014, an updated version of the PPWT was presented to the Conference on Disarmament by Russia and China (CD/1985, 2014). The updated PPWT contains a preamble and 13 Articles. The updated preamble emphasizes the commitment “not to threaten international peace and security by placing weapons in space or by transforming outer space in an area of military confrontation” (preamble, CD/1985). However, the updated preamble has been criticized for creating uncertainty regarding scope as any references to the right to explore and use outer space for peaceful purposes, as well as any direct references to arms control and disarmament agreements relating to outer space, have been removed (Tronchetti and Hao 2015).

The 2014 draft PPWT contains several notable changes from the 2008 version, including the removal of any definition of outer space. The definition of weapon in space has been slightly amended to mean:

any outer space object or its component produced or converted to eliminate, damage or disrupt normal functioning of objects in outer space, on the Earth's surface or in the air, as well as to eliminate population, components of biosphere important to human existence, or to inflict damage to them by using any principles of physics. (Article 1(b), CD/1985)

However, the definition of weapon in space remains a restrictive one. The challenge of properly defining weapon in space where so many space objects are dual-use is not effectively addressed in the 2014 draft PPWT. While the definition prohibits the deployment of any space object produced or converted for hostile purposes, the testing, deployment, and use of space objects for purposes such as active debris removal and near-Earth object diversion (which could easily be subsequently used as weapons) are not prohibited.

A space object is considered to have been placed in outer space if it “orbits the Earth at least once, or follows a section of such an orbit before leaving that orbit, or is permanently located in outer space or on any celestial bodies other than the Earth” (Article 1(c), CD/1985).

The definition of use of force and threat of force has been narrowed to:

any intended action to inflict damage to outer space object under the jurisdiction and/or control of other States, or clearly expressed in written, oral or any other form intention of such action. Actions subject to special agreements with those States providing for actions, upon request, to discontinue uncontrolled flight of outer space objects under the jurisdiction and/or control of the requesting States shall not be regarded as use of force or threat of force. (Article I(d), CD/1985)

This definition makes it clear that under the 2014 draft PPWT it would still be permissible for States Parties to test Earth-based ASAT technology on their own space objects. Article II remains the core provision of the 2014 draft PPWT and has been amended to read as follows:

States Parties to this Treaty shall:

- not place any weapons in outer space
- not resort to the threat or use of force against outer space objects of States Parties
- not engage in outer space activities, as part of international cooperation, inconsistent with the subject matter and the purpose of this Treaty
- not assist or incite other States, groups of States, international, intergovernmental, and any nongovernmental organizations, including nongovernmental legal entities established, registered, or located in the territory under their jurisdiction and/or control to participate in activities inconsistent with the subject matter and the purpose of this Treaty (Article II, CD/1985)

While explicitly recognizing the need for measures to verify compliance, Article V of the 2014 draft provides:



The States Parties recognize the need for measures to verify compliance with the Treaty, which may form the subject of an additional protocol.

With a view to promoting confidence in compliance with the provisions of the Treaty, States Parties may implement agreed transparency and confidence-building measures, on a voluntary basis, unless agreed otherwise. (Article V, CD/1985)

The USA opposed the 2014 draft PPWT, stating that “it does not address the significant flaws in its previous version, such as including an effective verification regime or dealing with terrestrially-based anti-satellite systems” (Rose 2014). As with the 2008 draft PPWT, the 2014 draft does not indicate what kind of transparency and confidence building measures states could take to ensure compliance with the treaty (Tronchetti and Hao 2015). The USA stated that there “is no integral verification regime to help monitor or verify the limitation on the placement of weapons in space. . . . Moreover, . . . it is not possible with existing technologies or cooperative measures to effectively verify an agreement banning space-based weapons” (CD/1998, 2014). The lack of a verification regime stands as a major impediment to the progress of the PPWT initiative (Su 2017). Russia and China responded that the Outer Space Treaty also does not provide any mechanisms for verification but that the development of verification mechanisms, to the extent possible, would be desirable for the full implementation of the PPWT (CD/2042, 2015). The USA also based its objections to the 2014 draft PPWT on the lack of a prohibition on “possession, testing, production, and stockpiling of such weapons” to prevent a Party from developing “a readily deployable space-based weapons break-out capability” (CD/1998, 2014). Russia and China responded that effective “monitoring of ‘research, development, production, and terrestrial storage of space-based weapons’ – on which there is no prohibition. . . – is not feasible in practical terms for objective reasons” (CD/2042, 2015). Additionally, the USA stated that the draft PPWT “does not address the most pressing, existing threat to outer space systems: terrestrially-based anti-satellite weapon systems. There is no prohibition on the research, development, testing, production, storage, or deployment of terrestrially-based anti-satellite weapons; thus, such capabilities could be used to substitute for, and perform the functions of, space-based weapons” (CD/1998, 2014). Russia and China responded that

While anti-satellite weapons as a class of weapons are not prohibited under the draft PPWT, the proliferation of such weapons is restricted through a comprehensive ban on the placement in outer space of weapons of any kind, including anti-satellite weapons. A ban on ground-based anti-satellite (ASAT) weapon systems has been introduced into PPWT through the ban on the use of force, regardless of its source, against space objects. (CD/2024, 2015)

Russia and China have further argued that ground-based ASATs are covered in the draft PPWT through the prohibition on the use of force and that the placement of weapons of any kind in outer space is prohibited (Chow 2018). Additionally, that there is a need to clarify the issue of the use of force in outer space on the grounds provided for in the Charter and to reach a common understanding of the right of self-defense under the Charter as regards outer space (CD/2042, 2015).

Although its provisions were substantially reworded, the 2014 draft PPWT retained the most criticized aspects of the 2008 draft PPWT (Tronchetti and Hao 2015). As the Conference on Disarmament requires consensus, it is unlikely that the PPWT will progress further given the ongoing opposition by the USA.

---

## International Code of Conduct for Outer Space

In 2008, the European Union (EU) released its proposal for an International Code of Conduct for Outer Space Activities (Code). While not legally binding, the Code was an attempt to establish “rules of the road” to enhance the safety, security, and sustainability of space operations (Koplow 2018). The initial draft of the Code was met with criticisms about the lack of consultation with other non-EU States. Informal bilateral consultations were then undertaken with Brazil, Canada, China, India, Indonesia, Israel, Russia, South Africa, the Republic of Korea, Ukraine, and the USA. This was followed by a series of multilateral consultations between June 2012 and May 2014, with meetings held in Vienna, Kiev, Bangkok, and Luxembourg (Johnson 2014). Several revised drafts of the Code were then released, with the latest version being released on 31 March 2014 (European Union, 2014 draft Code).

The purpose of the Code is to “enhance the safety, security, and sustainability of all outer space activities pertaining to space objects, as well as the space environment” (Article 1.1, 2014 draft Code). The Code “addresses outer space activities involving all space objects launched into Earth orbit or beyond, conducted by a Subscribing State, or jointly with other States, or by non-governmental entities under the jurisdiction of a Subscribing State, including those activities conducted within the framework of intergovernmental organisations” (Article 1.2, 2014 draft Code). The focus of the Code is directed less at the legality of weapons in outer space, and more at establishing rules of behavior and ensuring “transparency so that states can avoid accidental war in outer space” (Larsen 2017).

In the context of arms control and weapons in space, Article 4.2 provides that

The Subscribing States resolve, in conducting outer space activities, to:

- refrain from any action which brings about, directly or indirectly, damage, or destruction, of space objects unless such action is justified:
  - By imperative safety considerations, in particular if human life or health is at risk or
  - In order to reduce the creation of space debris or
  - By the Charter of the United Nations, including the inherent right of individual or collection self-defense

and where such exceptional action is necessary, that it be undertaken in a manner so as to minimize, to the greatest extent practicable, the creation of space debris

Article 4.2 does not expressly prohibit the deployment, research, or development of weapons in outer space and permits the use of such weapons in the

specific circumstances identified in the Article. Article 4.2 could be interpreted as permitting the use of Earth-based ASAT weapons in certain circumstances, where the use of such weapons is justified by imperative safety considerations, in order to reduce the creation of space debris, or in self-defense. The Code does not explicitly address space-to-Earth weapons in any way, which is potentially a significant shortcoming of the Code from a security perspective (Su 2017). The Code also does not address the challenges posed by dual-use space objects, nor does it specify what measures could be taken to verify compliance with the Code. Both Russia and China oppose the proposed Code, strongly preferring the treaty approach to arms control and the prevention of an arms race in outer space (Larsen 2017).

---

## Domestic Arms Control for Outer Space

In December 2019, the New Zealand government announced four policy principles which had been approved as an enhanced approach to payload permit assessments under the Outer Space and High-altitude Activities Act (Bradley 2019). In the context of arms control, under the updated policy the following payloads are banned from being launched into space from New Zealand:

- Payloads that contribute to nuclear weapons programs or capabilities
- Payloads with the intended end use of harming, interfering with, or destroying other spacecraft, or space systems on Earth
- Payloads with the intended end use of supporting or enabling specific defense, security or intelligence operations that are contrary to government policy
- Payloads where the intended end use is likely to cause serious or irreversible harm to the environment

These domestic restrictions on the launch of certain payloads may cover a broader range of weapons than the international space law regime.

---

## Conclusions

The Outer Space Treaty and the Moon Agreement both prohibit States Parties from placing nuclear weapons and other weapons of mass destruction in orbit, installing such weapons on celestial bodies, or stationing such weapons in outer space in any other manner. In addition, States Parties are prohibited from carrying out tests of weapons of any kind on celestial bodies. However, the current international space law regime does not prohibit (and so permits) states to develop conventional orbital weapons and Earth-based ASAT weapons.

The existing international space law regime addressing the potential weaponization of outer space is outdated, inadequate, and insufficient to adequately address arms control in outer space (Jaramillo 2009). An arms race in outer space, with states competing for control of space could “deter optimal patterns of peaceful exploitation of space, and even the current amplifying rhetoric about weaponization of space may make some wary potential space actors hesitant about investing in new space capabilities” (Koplow 2018). The rapidity with which space technologies are being developed and the increasing prevalence of dual-use space technologies which could also be used for hostile purposes, such as those used for active debris removal and near-Earth object diversion, challenge the existing space arms control regime, and remain an unresolved challenge for space arms control initiatives. One of the biggest challenges still to be overcome is definitional; the need for States to agree on a definition of what amounts to a weapon in space.

Arms control in outer space is not inherently more complicated or difficult than arms control in other domains (Koplow 2018), with the exception of verification challenges and the prevalence of dual-use objects in space compared to other domains. Any effective arms control regime for outer space must, by necessity, include all states (four as at the time of writing – the USA, Russia, China, India) that possess significant military arms technology that can be deployed in outer space (Larsen 2017). The problem is one of political will; “the resistance to effective arms control in outer space seems especially entrenched; even modest measures provoke a strong allergic reaction” (Koplow 2018). The USA has repeatedly stated that

The United States will oppose the development of new legal regimes or other restrictions that seek to prohibit or limit US access to or use of space. Proposed arms control agreements or restrictions must not impair the rights of the United States to conduct research, development, testing, and operations or other activities in space for US national interests. (Peoples 2011)

In contrast, Russia and China have repeatedly expressed a preference for treaty-based arms control measures to prevent an arms race in outer space. However, the international political and legal conditions for the acceptance of a new treaty regulating arms control and space security appear to be currently lacking, given that the international community has been unable to agree on a new treaty regulating space activities for more than 40 years (Tronchetti and Hao 2015).

As most states appear unwilling to accept binding restrictions on their ability to protect their space assets, any treaty-based arms control initiatives, such as the PPWT, appear unlikely to succeed. Consequently, nonbinding, soft law instruments may have the highest chance of advancing space security through states voluntarily adopting the best practice behaviors established. Arms control measures for space must be well-crafted, with adequate verification mechanisms and robust enforcement (Koplow 2018). Any arms control regime for space, whether hard or soft law, must be able to fill the normative void in the current space security treaty regime and reduce the risk of miscalculation and misinterpretation. Only in this way can space security be enhanced.

## References

- Agreement governing the activities of states on the moon and other celestial bodies. 11 July 1984. GA resolution 34/68, annex
- Bhat S, Mohan V (2009) Anti-satellite missile testing: a challenge to article IV of the outer space treaty. *NUJS Law Rev* 2(2):205–212
- Bradley G (17 December 2019) Government updates rules on what can be sent into space. *NZ Herald*. [https://www.nzherald.co.nz/business/news/article.cfm?c\\_id=3&objectid=12294704](https://www.nzherald.co.nz/business/news/article.cfm?c_id=3&objectid=12294704)
- Chow B (2018) Space arms control: a hybrid approach. *Strateg Stud Q* 12(2):107–132
- Delegation of the United States of America to the Conference on Disarmament. Analysis of the 2014 Russian-Chinese draft treaty on the prevention of the placement of weapons in outer space, the threat or use of force against outer space objects; conference on disarmament. CD/1998. 3 Sept 2014. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/007/57/PDF/G1500757.pdf?OpenElement>
- Draft treaty on the prevention of the placement of weapons in outer space and of the threat or use of force against outer space objects (2008) CD/1839 and (2014) CD/1985
- European Union (2014) Draft international code of conduct for outer space activities. [http://www.eeas.europa.eu/non-proliferation-and-disarmament/pdf/space\\_code\\_conduct\\_draft\\_vers\\_31-march-2014\\_en.pdf](http://www.eeas.europa.eu/non-proliferation-and-disarmament/pdf/space_code_conduct_draft_vers_31-march-2014_en.pdf)
- Hobe S, Schmidt-T B, Schrogl K.-U (eds) (2010) *Cologne Commentary on Space Law*, vol 1, Outer Space Treaty, Carl Heymanns Verlag, Köln
- Jaramillo S (2009) In defence of the PPWT treaty: toward a space weapons ban. *Ploughshares Monit* 30(4):11–14. [https://ploughshares.ca/pl\\_publications/in-defence-of-the-ppwt-treaty-toward-a-space-weapons-ban/](https://ploughshares.ca/pl_publications/in-defence-of-the-ppwt-treaty-toward-a-space-weapons-ban/). Accessed 26 Dec 2019
- Johnson C (2014) Draft international code of conduct for outer space activities fact sheet. Secure World Foundation, Washington, DC
- Koplow D (2018) The fault is not in our stars: avoiding an arms race in outer space. *Harv Int Law J* 59(2):331–388
- Larsen P (2017) Outer space arms control: can the USA, Russia and China make this happen. *J Confl Secur Law* 23(1):137–159
- López L (2012) Predicting an arms race in space: problematic assumptions for space arms control. *Astropolitics* 10:49–67
- Peoples C (2011) The securitization of outer space: challenges for arms control. *Contemp Secur Policy* 32(1):76–98
- Permanent Representative of the Russian Federation and the Permanent Representative of China to the Conference on Disarmament. Follow-up comments by the Russian Federation and China on the analysis submitted by the United States of America of the updated Russian-China draft PPWT. CD/2042. 14 Sept 2015. <https://documents-dds-ny.un.org/doc/UNDOC/GEN/G15/208/38/PDF/G1520838.pdf?OpenElement>
- Plath C (2018) Explanation of vote in the First Committee on resolution: L.50, “no first placement of weapons in outer space.” United Nations, 5 Nov 2018
- Rose F (2014) Statement by Deputy Assistant Secretary for Space and Defence Policy, Bureau of arms control, verification and compliance at conference on disarmament plenary session, 10 June 2014
- Shimabukuro A (2014) No deal in space: a bargaining model analysis of U.S. resistance to space arms control. *Space Policy* 30:13–32
- Su J (2010) The “peaceful purposes” principle in outer space and the Russia-China PPWT proposal. *Space Policy* 26:81–90
- Su J (2013) The environmental dimension of space arms control. *Space Policy* 29:58–66
- Su J (2017) Space arms control: lex lata and currently active proposals. *Asian J Int Law* 7(1):61–93
- Sullivan C (1990) The prevention of an arms race in outer space: an emerging principle of international law. *Temp Int Comp Law J* 4(2):211–237

- Treaty between the United States of America and the Union of Soviet Socialist Republics on the limitation of anti-ballistic missile systems, signed at Moscow 26 May 1972, entered into force 30 Oct 1972
- Treaty on principles governing the activities of states in the exploration and use of outer space, including the moon and other celestial bodies (10 Oct 1967) GA resolution 2222 (XXI), annex Tronchetti F, Hao L (2015) The 2014 updated draft PPWT: hitting the spot or missing the mark? Space Policy 33:38–49
- United Nations General Assembly (1963) Question of general and complete disarmament. GA Res 1884 (XVIII)
- United Nations General Assembly (1988) Prevention of an arms race in outer space. UN Doc A/RES/43/70
- United Nations General Assembly (2014a) Draft resolution on “no first placement of weapons in outer space.” UN Doc A/C.1/69/L.14
- United Nations General Assembly (2014b) No first placement of weapons in outer space. GA resolution 69/32
- United Nations General Assembly (2019) Further practical measures for the prevention of an arms race in outer space. UN Doc A/C.1/74/L.58/Rev.1



# Role of Space in Deterrence

# 7

John J. Klein and Nickolas J. Boensch

## Contents

Introduction .....	112
Space Deterrence .....	113
Deterrence by Punishment .....	114
Deterrence by Denial .....	116
Principles of Space Deterrence .....	119
Conclusions .....	125
References .....	125

## Abstract

A proper space strategy agrees with the universal and overarching logic of strategy. Therefore, the concept of deterrence has applicability in the space domain. Space activities and policies are relevant for deterring conflict, as well as maintaining international peace and stability. Although deterrence has a legitimate role in future space strategy, it is not the panacea for preventing conflict, because history teaches that deterrence will at times fail due to miscalculation, uncertainty, or chance. This is also true for deterring acts of aggression in space.

The views expressed in this article are solely those of the authors and do not necessarily reflect those of Falcon Research, the George Washington University, Bryce Space and Technology, or the US government.

---

J. J. Klein (✉)

George Washington University's Space Policy Institute, Washington, DC, USA  
e-mail: [kleinjj@gwu.edu](mailto:kleinjj@gwu.edu)

N. J. Boensch

Bryce Space and Technology, Alexandria, VA, USA  
e-mail: [nick.boensch@brycetech.com](mailto:nick.boensch@brycetech.com)

## Introduction

Secure access to space is a critical national security interest for many countries. Space-reliant technologies enable vital activities – including commerce, trade, environmental monitoring, intelligence collection, and governmental actions. Consequently, many countries will seek to ensure access to and use of space through diplomatic, informational, military, and economic instruments of national power. The strategic importance of space means that in a potential conflict, an adversary will be incentivized to blunt this advantage and challenge command of the domain. To discourage this behavior and protect one's national interests in space, the concept of deterrence is salient. The recent return of discourse focused on great power competition – fueled by Chinese belligerency in its territorial disputes and Russian adventurism on its borders and abroad – has a distinct space element and highlights that space deterrence will be a principal theme in space strategy for many space powers.

Since the beginning of the Space Age, some polities considered operations and activities in space as a means of supporting the ends of national policy. Thorough analysis of the nexus between space and deterrence, however, remained unexplored for decades largely for two reasons (Thomson 1995). First, space deterrence was considered to be closely coupled with nuclear deterrence thinking from the Cold War because space systems enabled nuclear command and control, supported early warning of ballistic missile launch, and served as national technical means of verification in arms control measures. Any interference against national security space systems was thought to be a potential precursor to a nuclear war. Second, in the immediate post-Cold War world, there was not a significant or explicit space threat to be deterred. China's 2007 direct ascent anti-satellite (ASAT) weapon test and subsequent military posture in space has been a catalyst that has prompted policy makers and strategists within the United States to more fully consider the role of deterrence in space strategy.

When developing space deterrence strategies, strategists should acknowledge the unity in strategic experience. The fundamental concept of deterrence is enduring and has been studied in depth. Just as Carl von Clausewitz identified the universal nature and changing character of war, the nature of deterrence is enduring, while its implementation differs between different domains of warfare and each geopolitical context (Clausewitz 1989). Consequently, when considering the role of deterrence in space, the strategist may use historical experience and lessons – from antiquity to the present day – to better understand the relationship between the space domain and deterrence theory. This chapter presents many of the most fundamental topics of space deterrence. Admittedly, much of the current literature on space deterrence focuses on the strategic challenges facing the United States; however, the lessons to be gleaned are often relevant to other countries. The concepts presented in this chapter are meant to guide readers and future strategists, thereby aiding them in thinking about deterrence in space and allowing them to identify sound arguments, train their judgment, and avoid pitfalls when crafting strategy (Clausewitz 1989).



## Space Deterrence

Fundamentally, deterrence efforts seek to affect the decision-making of others and influence their behavior. This is reflected in a commonly used definition that *deterrence* refers to persuading a potential enemy that it is in its own interest to avoid certain courses of activity (Schelling 1966). When a potential adversary forgoes certain actions or some forms of behavior that they would otherwise have carried out due to intolerable costs, this is commensurate with deterrence – through either denial or punishment. In its most simple form, deterrence involves persuading an adversary that the risks or costs of an action exceed any perceived benefit or gain.

Because states derive strategic advantages from satellites and potential rivals may seek to deny a state this advantage, the concept of “space deterrence” is a relevant concept for space powers. Deterrence by punishment, compellence, deterrence by denial, and dissuasion are important ideas in the formulation of a sound space strategy. Taking the commonly accepted definition mentioned previously, *space deterrence* refers to persuading a potential enemy that it is in its own interests to avoid certain courses of activity in, through, or from space. Regardless of the chosen terminology or definition, what is ultimately important is that there are actions that can be taken relative to space that affect the decision-making of others.

One of the most essential distinctions in deterrence theory is between deterrence by punishment and by denial (Snyder 1961). *Deterrence by punishment* concerns the threat of credible and potentially overwhelming force or other retaliatory action against any would-be adversary to discourage potential aggressors from conducting hostile actions. *Deterrence by denial* refers to the capability to deny the other party any gains from the behavior that is to be deterred (Snyder 1961). This concept refers similarly to deterring an adversary by presenting a credible capability to prevent it from achieving the potential gains adequate to motivate the action (Krepinevich and Martinage 2008).

A related but distinct concept is *compellence*, which involves convincing an adversary to cease some current undesired action. Compellence is often described as a direct action that persuades an opponent to give up something that is desired (Schelling 1966). While deterrence has a negative object – it discourages unwanted actions – the object of compellence is positive. Effort is expended to force or convince an actor to conform to one’s will.

Both military and nonmilitary means are applicable when seeking to affect the thinking of others to enable deterrence by punishment, deterrence by denial, and compellence. Nonmilitary means equate to the *soft power*, or the diplomatic, informational, and economic instruments of national power (Nye 2005). Nonmilitary means can be used to affect another state leader’s thought processes – whether reinforcing a currently held view that is beneficial to the deterring state or changing the view of another state’s leadership or politics. Consequently, a practical implementation of space deterrence may entail political and diplomatic efforts, such as new international treaties or agreements; multimedia stories presenting news in a favorable perspective; and commerce and trade activities that increase one’s own economic influence or affect negatively a potential adversary or opposing alliance (Klein 2019).

## Deterrence by Punishment

A deterrence by punishment approach in space is underpinned in the belief that the threat of credible and potentially overwhelming force or other retaliatory action against any would-be adversary is sufficient to deter most potential aggressors from conducting hostile actions in space. Such a strategy should clearly convey the capability and credibility behind the threat and communicate the specific behavior sought to be discouraged (Morgan 1977). As part of its broader space strategy, the United States seeks to deter attacks against its satellites. The 2017 US National Security Strategy conveys that harmful interference or attacks targeting US satellites will be met with a deliberate response in the “time, place, manner, and domain” of its choosing (The White House 2017). A US joint doctrine describes that, consistent with the right to self-defense, the United States may utilize its space assets to target the space capabilities of an adversary to deter potential threats (Joint Chiefs of Staff 2018). Some security experts view that the punishment portion of the US space deterrence strategy has been pursued and emphasized extensively, perhaps to the detriment of other approaches to secure US interests in space (Johnson-Freese 2017).

Many analysts have identified challenges associated with implementing a deterrence by punishment approach in the space domain. These include establishing appropriate thresholds for retaliation for both non-kinetic and reversible attacks on satellites, differences in severity due to no loss of life when compared to terrestrial action, and having the requisite attribution capabilities and processes.

The absence of explicit threshold that a state would retaliate against complicates efforts to deter adversaries. Some policy makers question whether non-kinetic and reversible actions are hostile acts or armed attacks that warrant a military response (Harrison et al. 2017). Reversible and non-kinetic actions on satellites supporting tactical operations may be treated differently from large-scale kinetic attacks on satellites supporting nuclear command or control or early warning missions. However, between these extremes, there is still a highly uncertain boundary that complicates deterrence efforts (MacDonald et al. 2016). Ultimately, what is considered an armed attack or hostile act in space necessitating a retaliatory response will depend on the broader geopolitical context.

Another challenge for a space deterrence strategy is that attacks on satellites typically are unlikely to result in loss of human life. Consequently, hostile actions in space may be considered by some polities to be less escalatory or grave as conflict on Earth. The frequently used adage that captures this thinking is “satellites don’t have mothers.” This view may cause decision-makers to view aggression in space as never rising to levels that would warrant a military response, whether terrestrially or in space. Moreover, because military actions in space are unlikely to produce direct casualties, there may be an appeal to turn to these activities as tensions between competing states escalate (MacDonald et al. 2016). Perceptions that hostilities in space are less severe than terrestrial conflict can be discouraging to those hoping to deter attacks against one’s satellites.

Regardless, the thought that the non-casualty-generating effects of space actions preclude a deterrent threat is unfounded. Article 2(4) of the United Nations Charter describes the need to refrain from the threat or use of force against a state's territorial integrity – which may be interpreted as a state's physical property. Self-defense and retaliatory threats to deter a potential armed attack against a state's satellites are then appropriate and justified. Upon further examination, one may dispel a historical challenge surrounding space deterrence by punishment: a hostile action against a state's space systems may still be deterred by threat of retaliation, even if there is no loss of life.

Yet another challenge to effective deterrence in space lies in the difficulty of attributing who or what caused a satellite to cease to function normally. Military actions in space can produce various effects, may be non-kinetic and reversible, and in some cases these effects may be difficult to identify and attribute. An effective deterrent requires timely assessment of the event to orient and respond appropriately. Operating at hundreds to more than 30,000 km above the Earth's surface makes it difficult to physically inspect and track satellites, thereby making determining and assessing damage an onerous endeavor. The hostile space environment – where satellites face solar activity, scorching and frigid temperatures, radiation, electromagnetic activity, and an increasing amount of debris – further complicates efforts (Wright et al. 2005). Operators must distinguish between intentional interference from adversaries and interference arising from normal operation in a hostile environment.

Some authors argue that the difficulties associated with attribution may be less worrisome than originally thought (Harrison et al. 2009). An attack on a state's satellites unconnected to a terrestrial strategic event is thought to be highly unlikely. Attacks on satellites will occur following the terrestrial breakdown of general deterrence between states. The source of an attack may be less nebulous than space deterrence literature has declared, particularly if the attacking state launches a coordinated attack on many satellites to try to gain command of space early in the conflict. Drawing from this example, intelligence gleaned prior to the attack may be a more meaningful method of attribution than enabled by postattack space situational awareness (SSA) assessment.

Regardless of this assessment, in the current context of the global proliferation of counterspace capabilities, there will likely be ample room for misperception and miscalculation in a state's leadership. This necessitates robust SSA capability to address issues of identifying, assessing, and attributing activities that occur in orbit. Greater SSA capabilities allow a state to differentiate between intentional attacks and malfunctions due to the satellite itself or the hostile environment it inhabits, thereby reducing the potential for misinterpretations and miscalculations (Sheldon 2008). Effective SSA capabilities will necessitate knowing what on-orbit systems are present, along with their location, capabilities, historical anomalies, operating patterns, and intended use. Such information will facilitate those preparatory measures needed to pit one's strengths against a potential adversary's weakness. Because SSA is a global endeavor, information sharing architectures must be designed to include

the international community and commercial industry. This means that much of the data and resulting information provided through SSA systems should be releasable and disseminated to many of those participating in the global effort.

Today's security challenges can complicate the implementation of a deterrence by punishment strategy. While some security analysts assess that thresholds for retaliation, differences in severity for space actions, and ensuring a sufficient attribution capability may be less problematic than many think, it remains to be seen whether this is confirmed in practice.

## Deterrence by Denial

Among many security professionals, *deterrence by denial* is often associated with the concept of *dissuasion* – activities that seek to influence the decision calculus of potential adversaries to discourage the initiation of military competition. A strategy incorporating dissuasion seeks to convey the futility of conducting a hostile act, affecting the confidence of a potential adversary's leadership and causing decision-makers to not pursue a military confrontation in the first place. To be most effective, dissuasion activities occur before a threat manifests itself. Some national security professionals note that dissuasion works outside the potential threat of military action as a kind of "pre-deterrence," because those states dissuaded will not require to be deterred by punishment (Krepinevich and Martinage 2008). While a deterrent that seeks to punish an adversary is tailored to distinct actions by specific actors at definite times, deterrence by denial commonly lacks this specificity and exists as a general deterrent, one that shapes the security environment through a broad, latent deterrent effect originating from one's reputation and capabilities (Morgan 1977).

A deterrence by denial strategy for space seeks to frustrate or complicate the adversary's plans by introducing greater costs and reducing associated benefit. Over the past several years, there has been a greater emphasis on the role of deterrence by denial in the broader US space deterrence strategy. Rather than threatening retaliation against the aggressor's satellites or terrestrial targets of value, a US space deterrence by denial strategy emphasizes reducing an adversary's incentive to attack US satellites (Vedda and Hays 2018). A potential adversary may be deterred if it concludes that an attack in space will be ineffectual in achieving the desired effect. Much of deterrence by denial and dissuasion necessitates preparing for potential conflict during peacetime. Because dissuasion involves discouraging the initiation of military competition, for the space domain the requisite peacetime preparedness is included within the contexts of *space mission assurance* and *resilience*.

According to the US joint literature, mission assurance entails a process to protect or ensure the continued function and resilience of capabilities and assets – including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains – critical to the performance of the Department of Defense mission essential functions in any operating environment or condition (Office of the Assistant Secretary of Defense for Homeland Defense 2015). Similar to mission assurance but with a different focus, *resilience* is an architecture's ability

to support mission success with higher probability; shorter periods of reduced capability; and across a wider range of scenarios, conditions, and threats, despite hostile action or adverse conditions (Joint Chiefs of Staff 2018). Resilience may leverage cross domain solutions, along with commercial and international capabilities. By definition, space mission assurance and resilience efforts can prevent a potential adversary from achieving its objectives or realizing any benefit from aggressive action. Space mission assurance and resiliency help convey the futility of conducting a hostile act and, consequently, enhance deterrence by denial and dissuasion efforts.

Space mission assurance efforts consist of *defensive operations*, which include off-board protection elements; *reconstitution*, which includes launching replacement satellites or activating new ground stations; and *resilience*, which includes on-board protection elements (Joint Chiefs of Staff 2018). Resilience in capabilities includes disaggregation, distribution, diversification, deception, protection, and proliferation. *Disaggregation* is the separation of dissimilar capabilities into separate platforms or payloads. *Distribution* utilizes a number of nodes, working together, to perform the same mission or functions as a single node. *Diversification* is contributing to the same mission in multiple ways, using different platforms, different orbits, or systems and capabilities of commercial, civil, or international partners. *Deception* is hiding one's strengths and weaknesses from one's adversaries. *Protection* is utilizing active and passive measures to ensure space systems provide mission support in any operating environment or condition. *Proliferation* is deploying larger numbers of the same platform, payloads, or systems of the same type to perform the same mission.

Space mission assurance may be supported by a number of preparations preceding a potential conflict. These preparations may include hardening against cyber threats and signal jamming, incorporating shutters for remote sensing satellites to minimize the effects of dazzling by lasers, or increasing the mobility of satellites through novel propulsion technologies (Kueter and Sheldon 2013). Preparations taken in peacetime may include employment of proliferated constellations of small satellites to complicate an adversary's space ambitions. Furthermore, the conduct and training of one's space and terrestrial forces may grant an ample deterrent effect, even if no ancillary preparations have been made. One method of frustrating an adversary's plans may be to train forces to fight under degraded conditions where military forces lose access to space-enabled capabilities, thereby depriving potential aggressors some of the appeal of attacking satellites (Harrison et al. 2009). Consequently, a potential aggressor may be convinced that the prospects for success are too costly, with little benefit.

Another method of frustrating an adversary's space control plans is to reduce one's vulnerability by transitioning traditional space-derived services to terrestrial alternatives, a concept termed *space avoidance*. Its advocates seek to increase space deterrence by minimizing one's presence in space, thereby diminishing an adversary's perceived benefits of attacking one's satellites (Coletta 2009). For example, some space avoidance advocates suggest this may be achieved by using unmanned aerial systems (UAS) for tactical reconnaissance systems instead of

remote sensing satellites. Creating redundancy through terrestrial alternatives is prudent, but one should not be misled when judging whether reliance on space can be abated entirely. UAS are a valuable supplementary resource to space-derived intelligence, surveillance, and reconnaissance (ISR); however, most UAS still require space-derived positioning information and communications to operate. Many forms of military power – sea power and airpower, for example – cannot easily reduce reliance on space-derived services. While states should seek to increase terrestrial redundancy to complicate an adversary's plans, a strategy of space avoidance intending to greatly reduce reliance on space is not feasible in modern warfare.

Alliances, international cooperation, and the global proliferation of space power also play a significant role in deterrence by denial. This international dimension influences deterrence in several ways. First, the proliferation of states operating or deriving benefits from satellites creates stakeholders who would likely prefer that their satellites were not put in jeopardy. States outside of the deterrence relationship may have their satellites affected negatively if deterrence fails and conflict ensues, such as by orbital debris from kinetic attacks or the indiscriminate effects of broad radio-frequency jamming. Second, the deterring state may provide a global or multinational space-derived service, such as the US Global Positioning System satellites, which if attacked could potentially draw countries reliant on this service into the conflict on the side of the non-aggressor (Harrison et al. 2009). In these situations, an aggressor may be hesitant to attack space systems if it will have to potentially contend with an international response (Sheldon 2008). Third, allied or partner states may assist the deterring state when a conflict breaks out. The space systems of friendly countries can complement and supplement the deterrer's own capabilities, such as through data sharing agreements, interoperability, or even by assisting in the reconstitution of lost space capabilities. Adversary leadership may be deterred from targeting US satellites if they perceive that the United States could leverage the capabilities of its allies to nullify any anticipated benefit (Sheldon 2008).

Some security experts consider the North Atlantic Treaty Organization (NATO) as being uniquely positioned to bolster deterrence in space through its cooperative alliance. The alliance is increasingly reliant on space for its collective defense and economic prosperity, and an attack on the space assets of any one ally impacts the security of all allies (Schulte 2012). Security experts assert that while NATO is dependent on space-enabled capabilities, its space doctrine and planning have not kept up. Presently, NATO officials are considering how the alliance should address the growing military capabilities of Russia and China, to include issuing NATO's first strategy for space. The strategy is expected to make space an official domain of operation, giving structure to discourse on military developments in space and NATO's response. The alliance may also decide that attacks in space would trigger the organization's Article 5 provisions on collective defense, although internal differences on the subject remain. Analysts have long held that NATO should continue to build the expertise and capacity to conduct operations enabled by space; ensure that doctrine, requirements, and planning account for the operational advantages provided by space; and adapt exercises and training to ensure forces can

effectively exploit space-based capabilities (Schulte 2012). It is still uncertain whether NATO's space strategy will implement these recommendations.

A deterrence by denial strategy presents its own challenges. The cost of fielding and launching the most robust, defensible space systems can become a financial burden (Coletta 2009). Hardened, dispersed, disaggregated, or diversified capabilities may cost more to develop, launch, integrate, and operate. Also, resilient architectures may not be able to match the performance of those exquisite space systems. In most cases, smaller, proliferated constellations of satellites will augment, rather than replace these exquisite systems. The space strategist then must consider the benefits of defensive approaches, along with associated time and fiscal procurement costs, when finally deciding upon the best approach. Another challenge of deterrence by denial is that one's space mission assurance and resilience efforts must be widely publicized to be effective in dissuading others.

Both deterrence by punishment and deterrence by denial are fundamental to an understanding of deterrence theory in space. Though deterrence can be valuable in one's attempts to prevent attacks and dissuade aggression, deterrence is not a panacea that will always prevent conflict. Clausewitz's wisdom is insightful. An adversary may strive to have the greatest likelihood of success by expanding its relative superiority, but even without this advantage, an adversary may find war attractive if there is no better option (Clausewitz 1989).

## **Principles of Space Deterrence**

Because deterrence is a strategic behavior, its fundamental nature is enduring, even though its implementation changes with time and for each geopolitical situation. To understand the role of deterrence in space, it is important to identify deterrence's most enduring concepts along with their relation to space strategy.

### **Primacy of the Adversary's Decision-Making**

A deterrence strategy is not a game of solitaire. All too often, policy makers and warfighters forget that those to be deterred may be unwilling or even unable to be deterred. Because war and deterrence are both within the realms of strategy, one must recognize that deterrence is a contest between two independent wills (Clausewitz 1989). The adversary's perceptions and decision-making are the paramount variables determining whether deterrence succeeds or fails. Regardless of the potential credibility of deterrence efforts, an adversary has an independent will and may not necessarily comply. Those to be deterred may fail to comprehend the threat or costs before them, doubt the credibility of the deterrent, or find that their policy ends are significant enough to warrant the costs and risks associated with ignoring the deterrence attempt (Sheldon 2008). Even if the deterring state has increased the costs and minimized adversary benefit through its defensive capabilities or with the demonstrated ability to respond, the decision to be deterred rests with the potential adversary.

Politics and their leadership cannot always be deterred, and they may decline to be coerced, even when heavily physically damaged, hoping for a change in strategic fortune (Gray 2007). “Fools,” as some may call them, are far more likely to commit errors of a kind that result in wars or at least a high measure of regional disorder, because they will not be swayed in their decision for violence regardless of the threat of a severe military response to a hostile attack (Gray 2007). In such situations, deterrence could be irrelevant, because the foolish foreign leader may not believe in the latent or explicit threats issued or may not care whether or not the threat of retaliation is honored. Sometimes, if the enemy has nothing to lose, even a very risky action may be preferable to maintaining the status quo. Ultimately, it does not matter whether one thinks a potential adversary should be deterred given an action or situation; it only matters how the adversary’s leadership and decision-makers interpret any action within their worldview and mental constructs. Regardless of the amount of political will and military strength behind a deterrent message, the potential adversary’s perceptions are what decide the success of a deterrence strategy.

### **Deterrence Cannot Be Guaranteed**

Strategic history demonstrates that one should be less than confident in the certainty of deterrence. It is possible, and perhaps even probable at times, that deterrence will fail. Ambiguity, miscalculation, incompetence, friction, and chance are all prevalent in deterrence and serve to ensure that deterrence is a highly uncertain venture. The primacy of the psychological aspects in this manifestation of strategy further adds to the uncertainty of deterrence (Sheldon 2008). There is the fundamental, persistent threat that the countries in a deterrence relationship will trip, accidentally or inadvertently, into war (Gray 1991). Some may be quick to forget that, much like war, deterrence is a strategic behavior and accordingly suffers from complexity, non-linearity, and unforeseeable occurrences that can thwart even the most careful and comprehensive planning. This complexity and nonlinearity should be considered and addressed when developing national strategies and operational plans.

One of the significant drawbacks of deterrence theory is identifying when it actually succeeds in causing an adversary not to proceed with an undesired behavior. Assessing the efficacy of deterrence is onerous because successful deterrence must be tested negatively with events that do not occur (Gray 1991). Because of the inability to draw convincing conclusions from events which did not happen, both the policy maker and strategist will likely be left with ambiguous lessons for the development of future strategies.

### **Credibility and Political Will Are Required**

Even with a sufficient capability to support affective deterrence, this capability can be rendered inconsequential if the deterring state lacks the will and credibility to carry out the deterring action (Sheldon 2008). Credibility is the perceived likelihood that the deterring state will follow through with its threat, if its terms are not obliged (Snyder 1961). There is a fundamental tension between credibility and prospective pain. Because of a rational fear of retaliation, the more painful or extreme a potential action is, the less likely it is to be taken, and the less likely it is that anyone will



believe it will be taken (Gray 1993). Credibility is dependent on the specific context of the security relationship, and effective credibility relies heavily on the political will of the deterring state to carry out its punitive actions.

While the possession of capability is essential, projecting the willingness to use punitive military force is paramount for deterrence to succeed (Schelling 1966). For this reason, there needs to be a belief that the political will exists to respond with severe military response if attacked in order for deterrence to work. One of the most dangerous scenarios is one in which the deterring state's determination to fight is underappreciated (Gray 1991). Having the requisite political will in using punitive action should deterrence fail is easily subject to misperception, and communicating political will does not inherently make it true or believed (Schelling 1966). Measuring the efficacy of projecting capability and political will, therefore, lies with those to be deterred.

### **Effective Communication Is Required**

Any effort to affect an adversary's decision-making is best served by clearly communicating one's desire, intent, capability, credibility, and rationale for military response. This requisite communication may be achieved through official statements or policy documents or more importantly through a demonstrated history of consistent actions (Klein 2019). If the deterring state is not clear in identifying the specific behaviors that it is trying to deter and conveying the threat of what will transpire if an aggressor chooses not to be deterred – along with the defensive capabilities mobilized to discourage them – then the prospects for successful deterrence are diminished. If one's deterrent message is not received or comprehended, then it will be difficult for deterrence to succeed (Schelling 1966).

In addition to the impediments in communicating deterrence in general, deterrence in space presents its own unique challenges that further complicate its potential success. The remoteness of space, highly classified nature of many of these systems, and perpetual concerns regarding dual-use technology all contribute to an environment where both sides of the deterrence relationship have limited awareness of or insight on the others behavior and conduct (Todd Harrison et al. 2017). Indeed, the dual-use nature of space systems can be particularly troublesome when attempting to clearly comprehend or communicate intent, because motive and intent are made more ambiguous when a state fields dual-use capabilities that can be used for civil, commercial, or military purposes.

Often in analysis of high-technology systems, capability is considered equal to intent (Gray 1993). While China is often at the center of debates over capability and intent, some security experts note the United States fields many of the same dual-use systems that elicit concern among its rivals (Johnson-Freese 2017). Intent is a frequently subjective matter and dependent upon one's worldview. For example, the Soviet Union viewed the US Space Shuttle program as a potential ASAT weapon because Soviet military leadership thought the Shuttle was capable of retrieving satellites and de-orbiting them (Wright et al. 2005). Assuming a worst case of intent based solely on an enemy's capabilities can raise the possibility of miscalculation and increase tensions among states when potentially none may be warranted.

To avoid any potential breakdowns in a deterrence strategy, clear communication of intent, credibility, capability, and what behaviors are sought to be deterred is paramount. While this would be difficult within the other domains, it is particularly important for deterrence in space.

### **Managing Escalation May Be Problematic**

Escalation is an especially complicated issue for the space domain, where an absence of historical experience of military conflict leaves the strategist with little empirical evidence to draw upon. Clausewitz explains the challenge of managing escalation, describing how the interaction of forces tends to drive war to the extreme (Clausewitz 1989). Schelling agrees, writing that escalation sets a pace that cannot be directly controlled (Schelling 1966). The propensity for conflict to escalate means that the space strategist should not act first without considering the potential repercussions of military action (Clausewitz 1989). As a result, prudence is necessary in the formation of a space strategy centered on deterrence.

Escalating horizontally into a different domain could result in much greater escalation than previously anticipated. For instance, a state's response to an attack on its satellites could involve terrestrial targets, thereby potentially causing casualties or violating another state's sovereignty. This horizontal escalation may be politically provocative and could drive further escalation. In many cases, militaries rely heavily on commercially procured and provided satellite services. Attacks against these commercial services could be seen as an inappropriate action that is escalatory to the international community.

### **Prospects for Strategic Misperception**

Strategic theory shapes how states prepare for and conduct strategy. This dimension then is pertinent when considering the execution of strategy. Understanding the strategic theoretical dimension calls for an appreciation, or at the very minimum recognition, of potential differences in interpretation of strategic theory of the adversary. Strategy mismatches – in which there are different cultural and social understandings in the theories of deterrence and escalation control – are some of the most dangerous situations between states. This danger arises because states, whose leaders may consider themselves to be rational and reasonable in not seeking direct military confrontation, may find themselves in such a war, despite their intent or desire. Because of the different understandings of deterrence in preventing war or deterrence's ability to control escalation during conflict, it is important to underscore the differences between American and many Western countries' views and the perceptions of Russia and China. The Russian military's strategy of "escalate to de-escalate" and the Chinese view of using "compellence" through military actions to avoid conflict are two strategic approaches to deterrence that are not emphasized in Western views on deterrence but must be well understood by policy makers and strategists.

In describing *strategic deterrence*, Russian military writings describe the term as an approach seeking to induce fear in opponents, whether in peace or war.

Therefore, the concept includes elements of what others may call *deterrence*, *containment*, and *coercion* (Fink 2017). Russia's approach to deterrence is grounded in its understanding of internal and external threats, including a sense of military asymmetry compared to the West. Russian military doctrine describes perceived dangers from the United States and NATO readiness to use military force, instability and terrorism that could challenge Russia's sovereignty, and a local conflict on its vast borders that could escalate into hostilities, which could include the use of nuclear weapons (Klein 2019). In the Russian perspective, strategic deterrence is not entirely defensive. Within US security circles, some may consider Russia's view of strategic deterrence as an "escalate to de-escalate" strategy – even though that term is not used within Russian military doctrine or strategies – because the strategy comprises the use of military force and actions to potentially de-escalate hostilities or tensions (Schneider 2017). The Russian concept transcends a traditional perception of deterrence having failed if conflict erupts. Therefore, deterrence can continue to work in times of war to prevent escalation, to ensure de-escalation, or for the swift termination of conflict on terms acceptable to Russia.

As with Russia, the Chinese concept of deterrence is fundamentally different than American and Western thinking. Analysis of Chinese writings notes the Chinese concept of deterrence includes a significant element of compellence and coercion; therefore, Chinese deterrence goals may include actions seeking to intimidate the opponent through economic, diplomatic, or military coercion in a way that directly affects an opponent's interests in order to compel the foe to submit to Beijing's will (Kaufman and Hartnett 2016). As a result, the Chinese see deterrence as having a positive object for achieving political ends, whereas the West typically places emphasis on the negative object of deterrence: the discouragement of actions. There are nuances in the Chinese terms used, especially those with more coercive connotations.

Chinese strategists view escalation not as a risk to be avoided but a means to manipulate an adversary (Lewis 2018). China also places special emphasis on overwhelming an opponent through rapid escalation, an approach that – when coupled with manipulation of an opponent's perceptions of the costs of a conflict through coercive measures – increases the chances for dangerous misperceptions. Chinese writings note that along a continuum of conflict, there may be scenarios where militaries are involved but war has not yet formally broken out (Kaufman and Hartnett 2016). Differences between Chinese and American views of deterrence include the Chinese focus on compellence, including coercion, rather than solely on dissuasion. Therefore, the Chinese idea of deterrence manifests itself in both coercive and dissuasive terms (Cheng 2018).

Differences in deterrence theory among Russia, China, and the United States are significant in how they may manifest in practice. Russia's emphasis on harnessing escalation to its advantage and Chinese views on compellence, military activities short of war, and rapid escalation create opportunities for misperceptions and potentially an irreversible slide into conflict that no state desires. These strategy mismatches also have implications for space deterrence because they demonstrate

how states may approach deterrence in this domain differently, potentially in ways that make it more likely that conflict will occur.

### **Space Deterrence Has a Terrestrial Aspect**

While this chapter focuses on space deterrence, it is essential to emphasize that deterrence and prospective conflict in space do not occur in isolation from a political and terrestrial context. This has two implications for space deterrence. First, even when there are times of significant instability in the space domain between two powers, the broader strategic landscape of inherent stability within other domains may restrain the initiation of conflict in space (MacDonald et al. 2016). Alternatively, a stable space environment could witness conflict if instability in other domains caused deterrence efforts to break down between rival space powers. Second, deterrence by punishment strategies attempting to prevent aggressive behavior in space is not limited in their targeting to the space environment. A strategy of space deterrence could succeed if it threatened terrestrial assets valued by the potential aggressor, and not necessarily just their space systems, a view that corresponds with the 2017 National Security Strategy. Therefore, there are complex interdependencies that exist between space and terrestrial domains in the effective implementation of a space deterrence strategy.

Space strategy indirectly influences general deterrence by enhancing the lethality of terrestrial forces and by increasing transparency in a deterrence relationship between competing states.

Space-based or space-enabled communications, surveillance, early warning, and navigation services can enable better coordination, communication, logistics, and superior situational awareness to terrestrial forces, thereby enhancing these terrestrial forces' response time, tempo, and operating efficiency. Space-enabled forces can typically engage an adversary with greater speed, precision, and coordination when compared to forces that lack sufficient command of space. Some analysts assess that the strategic effect accorded by space capabilities shifted the basis of US deterrence strategy from the threat of nuclear punishment to denial of the adversary's conventional offensive success (Coletta 2009). Space-enabled capability is thought to give a state's military the ability to increase the lethality and efficacy of its forces, which can in turn create a powerful deterrent to a would-be adversary. Many within China and Russia believe that US space-enabled conventional forces can cripple the command and control of their forces, even without the use of nuclear weapons (Lewis 2018).

Space also contributes to deterrence by creating transparency between adversary states. Space-based systems' global and nearly ubiquitous nature allows satellites to peer into the normally opaque actions of states and provide greater insight to decision-makers (Smith 2016). Satellites' freedom of overflight creates transparency between states, which is essential for deterrence to succeed. This information and knowledge help alleviate some of the unfounded fears between states and may aid in preventing strategic miscalculations. It must be emphasized that space-based capabilities do not allow one to be privy to thoughts and intentions of an adversary, and consequently, uncertainty will persist, even if mitigated to some degree (Smith 2016).

## Conclusions

Space imparts many strategic benefits that enable the military and nonmilitary activities of states. The strategic effect derived from space-based capabilities will not remain unchallenged when states drift toward war. Consequently, space powers will likely seek to implement a practical space deterrence strategy to protect their national interest and achieve political ends. Even though deterrence has a legitimate role in future space strategy, it is not the panacea for preventing conflict. Strategic history teaches that deterrence will at times fail due to miscalculation, uncertainty, or chance – ideas incorporating the concept of Clausewitzian friction. This may also be the case for deterring acts of aggression in space, especially considering China, Russia, and the United States have different perspectives on deterrence and escalation control. Facing recent nefarious activities of China and Russia, security commentators in the United States now emphasize a return to great power competition. Space has a unique role in this competition because all three great powers are also great space powers that seek to broaden their use of space while also fielding capabilities to contest command of this domain. Space deterrence will then play an important role within the global community in the future.

Albeit this chapter has emphasized the enduring nature of war and strategy (and therefore deterrence), the character of war changes with time. The implementation of space deterrence should also be expected to change. This change is currently reflected by the growth of the commercial space sector (particularly in the United States, Europe, China, and Japan) – whether in reusable or responsive launch vehicles or mega-constellations of Earth imaging and communications satellites. Studies of space deterrence often omit the potential role of the burgeoning commercial space sector. The exponential growth in commercial capabilities means that denying space services or degrading another's access to or use of space will become even more challenging for great space powers. The commercial space industry can help convey the futility of conducting a hostile act in space, because it will be difficult to deny products or services through a hostile action. This fact may cause a potential adversary's leadership to avoid military confrontation in the first place. Therefore, deterrence by denial may play a greater role than deterrence by punishment during future strategic deliberations than it has to date. This situation is an advantageous development, because governments can focus less time and resources on fielding military-related programs for use in times of conflict, instead giving more support to those commercial services and capabilities that can be used for the benefit of all.

---

## References

- Cheng D (2018) Evolving Chinese thinking about deterrence: what the United States must understand about China and space. The Heritage Foundation
- Clausewitz C von (1989) On war (trans and ed: Michael Howard and Peter Paret). Princeton University Press, Princeton
- Coletta D (2009) Space and deterrence. *Astropolitics* 7(3):171–192

- Fink A (2017) The evolving Russian concept of strategic deterrence: risks and responses. *Arms Control Today* 47
- Gray C (1991) Deterrence resurrected: revisiting some fundamentals. *Parameters* 21:40–47
- Gray C (1993) *Weapons don't make war: policy, strategy, and military technology*. University Press of Kansas, Lawrence
- Gray C (2007) *Fighting talk: forty maxims on war, peace, and strategy*. Greenwood Publishing, Westport
- Harrison R, Jackson D, Shackelford C (2009) Space deterrence: the delicate balance of risk. *Space Def* 3(1):1–30
- Harrison T, Cooper Z, Johnson K, Roberts T (2017) *Escalation and deterrence in the second space age*. Center for Strategic and International Studies, Washington, DC
- Johnson-Freese J (2017) *Space warfare in the 21st century: arming the heavens*. Routledge, Abingdon
- Joint Chiefs of Staff (2018) *Space operations*. Joint Publication 3–14
- Kaufman A, Hartnett D (2016) *Managing conflict: examining recent PLA writings on escalation control*. CNA, Arlington
- Klein J (2019) *Understanding space strategy: the art of war in space*. Routledge, Abingdon
- Krepinevich A, Martinage R (2008) *Dissuasion strategy*. Center for Strategic and Budgetary Assessments. <https://csbaonline.org/research/publications/dissuasion-strategy>
- Kueter J, Sheldon J (2013) *An investment strategy for national security space*. Special report no. 129. The Heritage Foundation
- Lewis J (2018) “Bottom line thinking” about the “Commanding Heights”. In: Wright N (ed) *Outer space; earthly escalation? Chinese perspectives on space operations and escalation*. NSI, Boston
- MacDonald B, Blair D, Cheng D, Mueller K, Samson V (2016) *Crisis stability in space: China and other challenges*. Foreign Policy Institute, Washington, DC
- Morgan P (1977) *Deterrence: a conceptual analysis*. Sage Publications, Beverly Hills
- Nye J (2005) *Softpower: the means to success in world politics*. Public Affairs, New York
- Office of the Assistant Secretary of Defense for Homeland Defense (2015) *Space domain mission assurance: a resilience taxonomy*. <http://policy.defense.gov/Portals/11/Space%20Policy/ResilienceTaxonomyWhitePaperFinal.pdf?ver=2016-12-27-131828-623>
- Schelling T (1966) *Arms and influence*. Yale University Press, New Haven
- Schneider M (2017) *Escalate to De-escalate*. U.S. Naval Institute Proceedings. <https://www.usni.org/magazines/proceedings/2017-02/escalate-de-escalate>
- Schulte G (2012) *Protecting NATO's advantage in space*. *Transatlantic Current* (5). National Defense University. [www.dtic.mil/dtic/tr/fulltext/u2/a577645.pdf](http://www.dtic.mil/dtic/tr/fulltext/u2/a577645.pdf)
- Sheldon J (2008) *Space power and deterrence: are we serious?* The George C. Marshall Institute. Policy Outlook
- Smith MV (2016) *Space power and the strategist*. In: Bailey R Jr, Forsyth J Jr, Yeisley M (eds) *Strategy: contest and adaptation from Archidamus to airpower*. Naval Institute Press, Annapolis
- Snyder G (1961) *Deterrence and defense*. Princeton University Press, Princeton
- The White House (2017) *The national security strategy of the United States of America*
- Thomson A (1995) *Satellite vulnerability: a post-cold war issue?* *Space Policy* 11(1):19–30
- Vedda J, Hays P (2018) *Major policy issues in evolving global space operations*. The Mitchell Institute for Aerospace Studies
- Wright D, Grego L, Gronlund L (2005) *The physics of space security a reference manual*. American Academy of Arts and Sciences, Cambridge



# Resilience of Space Systems: Principles and Practice

# 8

Regina Peldszus

## Contents

Introduction .....	128
Resilience as Concept in Space Security Policy .....	129
Resilience for Deterrence in an Emerging Threat Environment: US Perspective .....	129
Resilience for Critical Infrastructure Protection and Non-dependence: European Perspective .....	131
Resilient Architecture and Infrastructure: The Mission Assurance and Deterrence Perspective	132
Resilience as Key Quality of Functional Architecture .....	132
Functional Elements of Resilient Architecture .....	133
Practical Measures .....	134
Trading Off Resilience and Capability in Architecture .....	134
Resilient Operations and Organizations: The High Reliability and Resilience Engineering Perspective .....	135
Resilience Through Sensemaking .....	136
Resilience Through Performance Variability .....	138
Practical Measures .....	138
Assessing Resilience in Operations and Organizations .....	139
Disciplines Contributing to Resilience .....	139
Resilience Through Space Situational Awareness .....	140
Resilience Through Transparency Measures and Partnerships .....	140
Resilience Through Foresight .....	141
Conclusion .....	141
References .....	142

## Abstract

In view of the increasing complexity of the space environment, resilience has emerged as a pervasive concept in contemporary space security. This chapter provides an overview on the principles and practice of resilience of space systems

R. Peldszus (✉)

Department of Space Situational Awareness, German Aerospace Center (DLR) Space Administration, Bonn, Germany  
e-mail: [regina.peldszus@dlr.de](mailto:regina.peldszus@dlr.de)

and operations. It frames the emerging field from two distinct but complementary approaches: mission assurance and deterrence and high reliability and resilience engineering. Drawing on contemporary thinking from civilian and military perspectives, the chapter posits resilience as a distinct yet malleable notion at the intersection of space security and safety and highlights specific areas meriting further engagement for policy makers, systems analysts, and operators.

---

## Introduction

In the past decade, the concept of resilience has come to the fore in contemporary space policy and systems development as a critical quality of space infrastructure and a prerequisite for space security (Pace 2015). As the utilization of the orbital environment transforms, space assets are becoming increasingly exposed to the hazards and dynamics of ever more heterogeneous activity.

Situated within a complex operational domain, space systems are highly complex themselves. Characterized by nonlinear, interdependent interactions and tight coupling, they are prone to incidents or failure (Perrow 2007). Specifically, the bespoke exquisiteness of spacecraft and fleet of spacecraft – the current paradigm of communications, positioning, navigation, timing (PNT), and Earth observation systems – makes them susceptible to internal and external disturbance that includes a hostile physical environment with extreme temperature changes and radiation but may also be posed by operational constraints, mishaps, and, as it is increasingly asserted, the potential of adversary threat.

In view of this “brittleness” or fragility, strategic planners increasingly advocate rendering systems more resilient. (The terms “resilience” and “resiliency” are used synonymously in the relevant body of thought and practice across the sector; for the purpose of this chapter, “resilience” will be used to denote both.) Depending on domain and methodological vantage point, resilience in highly complex large-scale sociotechnical systems refers to the ability to withstand disturbance, bounce back from failure, and continue operations under varying conditions through qualities such as robustness, redundancy, resourcefulness, flexibility, survivability, and contingency planning (Haimes 2009, here 496; Air Force Space Command 2016). Whether articulated as a property or process (cf. sections “[Resilient Architecture and Infrastructure: The Mission Assurance and Deterrence Perspective](#)” and “[Resilient Operations and Organizations: The High Reliability and Resilience Engineering Perspective](#)”), resilience essentially manifests the *state* of a given system and its subsystems to respond to specific threats, and addressing through physical configuration, operation, and organization is understood as integral to risk management processes (Haimes 2009).

This chapter maps out the conceptual notions of resilience specifically for the space domain. In adopting a distinction parallel to that of security in and from space, focus is placed on resilience *in* space, or of space systems, which here refers to both the space and ground segment.

There is currently no generally agreed nomenclature in the community of practice for defining, describing, implementing, and assessing resilience in space. At the



same time, emerging frameworks for the resilience of space systems are not yet widely shared, and their applicability is often tailored to the specific sub-domain they have been conceived to address, i.e., military or civilian system. Charting the notion of “resilience” in the space domain therefore requires casting a wider net in the safety and security sciences and relating already consolidated concepts to emerging formulation in the context of space security.

Two major perspectives on resilience in space currently inform policy making and implementation: on the one hand deterrence and mission assurance and on the other resilience engineering and high reliability organizing. The following first outlines how these strands feature in discussions on resilience in contemporary space security policy and then addresses them in detail with regard to how they theoretically and practically relate to space architecture and infrastructure and organization and operations. Disciplines contributing to resilience in space are then highlighted, and a conclusion suggests issues meriting further attention in the immediate future.

---

## **Resilience as Concept in Space Security Policy**

As space actors explore future directions in a changing and complex domain, the notion of resilience has lodged itself firmly as an important element in developing space policy. However, despite its pervasive invocation as an end of policy efforts – both to render space systems more resilient and ensure societal resilience through space infrastructure and services – the terminology and approaches to resilience are little consolidated in theory, deconstructed for practical application, or subject of a sustained discourse akin to that for resilience in other domains such as aviation or offshore operations. In the past years, two major conceptual directions have begun to emerge in the USA, Five Eyes community, and Europe, which represent discrete approaches that are mutually complementary.

## **Resilience for Deterrence in an Emerging Threat Environment: US Perspective**

Resilience first surfaced prominently in the US Space Policy of 2010, whose objectives included “increas[ing] assurance and resilience of mission-essential functions” (Arnold and Hays 2013, here 121). The idea was broken down into the development of instruments, structures, and capabilities required for the continuity of space-based services in view of a “degraded, disrupted, or denied space environment,” and mechanisms to ensure that requirements for mission assurance and space system resilience would be addressed during acquisition processes for future space capabilities (US National Space Policy 2010, here 9).

In response to disruptive changes in the orbital environment – specifically with regard to new state actors with capabilities that increasingly included a repertoire of technology that could be used for offensive actions – resilience was posited as one of

the key approaches to maintaining superiority in space (Pawlikowski et al. 2012): if it were evident to a potential adversary that a system would bounce back from attack, or the damage inflicted would either be recovered swiftly or have limited repercussion on the overall capability afforded through a system or architecture, this would change the calculus of an adversary to attack. The aim was hence a resilient architecture that would be able to “support the functions necessary for mission success with higher probability, shorter periods of reduced capability, and across a wider range of scenarios, [environmental] conditions, and threats, in spite of hostile action or adverse conditions” (DOD 2012, here 4 and 14). Designing and maintaining a resilient system that would withstand and recover would thus mitigate or deny an adversary the benefit of attack (ibid.). In this sense, resilience formed a fundamental element of layered deterrence (Johnson-Freese 2016).

The US approach to framing and creating taxonomies for resilience in space to this date draws predominantly on the defense vantage point. This is also reflected in the space policies of the Five Eyes community. Here, the focus on architecture and capability subtly shifts to missions or infrastructure but in a similar context of sovereignty, emerging threats, and the terminology of a “congested and contested” domain, whereby resilience would serve as countermeasure against adversarial activities to “disrupt, degrade, or damage” (A New Space Strategy for Canada 2019, here 16; National Space Policy 2015). While not all space policies of the Five Eyes explicitly echo the US concept of resilience in these specific terms, their strategies and reasoning are supported by language to that effect: in placing emphasis on the need for space security, they focus on pillars regarded as contributors to resilience in US space policy, such as international partnerships and Space Situational Awareness (see also section “[Disciplines Contributing to Resilience](#)”) (cf. the space strategies, respectively policies, of New Zealand and Australia).

The dedicated UK Space Security Policy (2014) further draws on resilience as element of its definition of space security per se. It highlights a dedicated approach with regard to becoming resilient in view of concrete disruptions, both human-made and natural. To this end, the overall goal of resilience of space capabilities and services is diversified into several objectives (ibid., here 4). These include the pursuit of a “proportionate approach to investing in resilience, balancing protective measures with other means [...] such as alternative or fallback capabilities” that allow for continued availability of services, with the aim of “enhance[ing] the resilience of essential services [...] to the disruption of satellite operations”; and the commitment to “work with [other partners including the US, EU, EU Member States, and ESA] on an integrated approach to security in European space programs [...] including infrastructure and systems resilience” (ibid.).

By emphasizing disruption rather than threat and deconstructing resilience in business continuity terms that dovetail with the nomenclature used by a wide range of stakeholders including commercial industry, the UK policy already uses a number of concepts that resonate with a civilian-rooted approach more prevalent in Europe.

## Resilience for Critical Infrastructure Protection and Non-dependence: European Perspective

Recent European perspectives on resilience in space reflect US policy to a large degree, albeit on a higher level of abstraction and by situating resilience at the intersection of a multifaceted interpretation of space security, reliability, and safety. They place greater emphasis on space-based systems as critical infrastructure, rather than prominently as means of force projection, space control, and dominance or superiority. Instead, resilience is presented and proposed through a prism of views including civil protection, continuity of services, strategic non-dependence, and autonomy, as necessary measures in response to asymmetric and hybrid threats, as means to foster the synergy of civil and military capabilities or a robust industrial base, and as societal protection from natural hazards (cf. Robinson et al. 2018; ESPI 2018; Pellegrino and Stang 2016, here 8; cf. also ESA's proposed Space Safety program).

National space policies in Europe can be positioned on this spectrum. The French space defense strategy explicitly situates resilience as a central consideration of strategic, operational, and space systems development efforts in view of adversaries' offensive counterspace capabilities (Ministère des Armées 2019). The current German space strategy does not refer to resilience, but the government's overarching security policy deliberations identify resilience of space systems – as critical infrastructure – as fundamental need in the context of hybrid threats (BMVg 2016, pp. 58, 60). Other European space policies do not employ the concept of resilience but draw on compatible concepts, such as reliability, continuity, and access to space, and dedicate considerable attention to laying out specific elements conducive to resilience, such as international partnerships and Space Situational Awareness (cf. the space policies or strategies of Italy, Norway, and Sweden).

On a supranational level, the distinct element of European non-dependence in view of third-party capabilities surfaces, which echoes sovereignty concepts in the US deterrence context. As part of its four strategic goals, the European Union's Space Strategy (European Commission 2016) ascribes to “resilience of critical European space infrastructure” a central role as catalyst to reinforce European autonomy in space access and utilization, by ensuring the “protection” and “integrity” of the flagship programs for navigation and Earth observation, Galileo and Copernicus (here 8–9, cf. also European Defense Action Plan). To this end, and analogous to the USA, the specific measure of consolidating diverse European Space Situational Awareness capabilities is proposed; their current transformation into a dedicated program articulates distinctly civilian terms but accommodates considerable leeway in extending both operational and research and development efforts to a wider range of hazards and threats.

Beyond the specific reference to Space Situational Awareness (SSA) as a driver – and apparent placeholder – for resilience, the concept for resilience is neither fleshed out theoretically in European space policy in further detail nor translated into concrete activities or instruments for assessment and evaluation.

Indeed, the development of a dedicated methodological framework has been pointed out as a necessary element for further discussion (Pellegrino and Stang 2016). Yet, on a higher level in the context of EU foreign and security policy, the idea of resilience has become an overall *leitmotif* and guiding principle in the evolution of shared structures that allow averting external risks and threats (Bendiek 2017, here 14). Similarly, the upcoming NATO space policy can be expected to employ language on resilience, given its increasing awareness of the space domain and an overall stance on addressing hybrid warfare (cf. Prior 2017).

Regardless of the idiosyncratic nuances that are being emphasized in the integration of resilience into space security policy and the level of maturity of the related discourse, there is nascent understanding of the various elements for application in space systems, both in architecture and operations.

---

## **Resilient Architecture and Infrastructure: The Mission Assurance and Deterrence Perspective**

Extending the scope of policy, a limited but growing body of work exists on deconstructing the concept of resilience into applicable elements for space. One approach, departing from the perspective of assurance and deterrence as outlined previously for US space policy, involves describing discrete measures that can be practically applied in space systems and guide their development.

### **Resilience as Key Quality of Functional Architecture**

In response to the National Security Space Strategy from 2011, and in explicit recognition of the lack of a commonly shared taxonomy to facilitate a discussion on resilience and an approach to measuring it, resilience was fleshed out further through a dedicated taxonomy (OSD 2015). The concept was structured specifically through the lens of mission assurance in the warfighting rather than systems engineering domain, focusing on space-based and ground-based infrastructure. (This was contextualized by highlighting the overall assurance afforded by being able to switch to an alternative domain outside space, which was, however, not subject of the taxonomy effort.) Thus, “Space Domain Mission Assurance” was defined as distinct pillars that flanked resilience between defensive operations and reconstitution (*ibid.*, here 3 and following):

- *Defensive Operations* (disrupting an adversary’s ability to target; direct intercept; systematic maneuvering to avoid, confuse, or overwhelm a targeting system; active measures to deceive, degrade, or destroy a targeting system)
- *Reconstitution* (providing backup capacity by launching additional satellites or providing additional ground stations; replenishing parts of a constellations; add new signals or spectrum)

- *Resilience* (an to support “functions necessary for mission success with higher probability, shorter periods of reduced capability . . . in spite of hostile action or adverse conditions”)

The taxonomy emphasizes that, rather than resilience per se being the primary goal of an assurance effort, “it is the warfighting mission assurance benefit, derived from resilience, which [it] seek[s] to assure” (ibid., here 2). As a *means* for assurance rather than an inherent overall goal of a system, resilience is understood as an “internally focused characteristic” – a critical quality or property of a capability that helps ensure its continued availability, reliability, and integrity.

## Functional Elements of Resilient Architecture

Much of the discussion on mission assurance was initially centered on the concept of disaggregation as one approach to achieve or improve resilience (Air Force Space Command 2016). Disaggregation here meant the “dispersion of space-based missions, functions or sensors across multiple systems” (ibid., here 3). This would entail five disaggregation approaches, including *modular decomposition* within a single system to allow, e.g., individual subcomponent replacement; *functional* disaggregation by distributing sub-missions on separate platforms, including *hosted payloads* on assets of different missions or agencies; *multi-orbit* disaggregation that employs multiple orbital planes; and *multi-domain* disaggregation, whereby space-based and ground-based systems cooperatively or complementarily perform a mission. From a general resilience viewpoint, disaggregation resonates with the fundamental notion of deconcentration of critical or exposed capabilities for target reduction, which constitutes a paramount approach to addressing vulnerabilities of large-scale socio-technical systems (Perrow 2007, here 6 and 261).

However, for the space domain, additional – and partially overlapping – dimensions beyond disaggregation were being explored. Distribution, dispersion, and diversity by leveraging the capabilities of government and commercial stakeholders, increasing the number of platforms, and focusing on hosted payloads and mixed architectures were advocated early on as architectural – and hence also acquisitions-related – responses to the contemporary challenges faced by the traditional class of aggregated, highly integrated assets with long lifetimes (Pawlikowski et al. 2012).

Eventually, the focus of policy makers shifted from disaggregation toward a wider context of space protection after the 2014 Space Strategic Portfolio Review (cf. Johnson-Freese 2016, here 171; McLeod et al. 2016, here xii). Resilience itself was broken down into six characteristic architectural “sub-elements,” systematically defining several concepts that had been shown as partially interrelated elements previously (OSD 2015) (Here slightly changed in order of appearance for easier comparison):

- *Disaggregation*, the separation of dissimilar capabilities into separate platforms and payloads, thereby in cases also reducing overall complexity of the system

- *Distribution*, by employing a number of nodes that jointly perform the same function of mission as a single node, allowing for graceful degradation despite failure of a single node
- *Diversification*, by employing different platforms, orbits, systems or actors' capabilities to contribute to the same mission; flexible or adaptable systems
- *Proliferation*, by deploying larger numbers of the same [similar] platforms, payloads, or systems of the same types to perform the same mission
- *Protection*, through active and passive measures including protection from jamming, nuclear hardening, extended maneuverability, internal hosted decoys, onboard countermeasures, onboard/operational event characterization or attribution efforts/instruments
- *Deception*, through measures to confuse or mislead regarding location, capability, operational status, mission type, robustness of system/platform or payload; measures at architectural, operational, or organizational level

While deception was identified explicitly as “a critical element of any space system resilience effort,” all elements need not necessarily be present in a single architecture but rather enhance resilience cumulatively or in combination (*ibid.*, here 8).

## Practical Measures

A wide range of detailed practical measures can be mapped onto these elements for different levels of space systems. (Note that this selection of practical aspects dovetails with the concepts outlined in the next section.) On the platform level, this may include the hardening and shielding against radiation and kinetic and non-kinetic manipulation; fitting bimodal receivers for different navigation systems or equipping the spacecraft with measures for easier tracking; increased onboard autonomy for measures such as passively safe trajectories during proximity operations; reactive maneuvering in view of another approaching object; and cyber protection to safeguard commanding and telemetry. In the ground segment, there are a number of measures ranging from situating facilities in remote areas for limiting discovery, access, or interference; installing backup facilities; ensuring interoperability with legacy, novel, and partner infrastructure; and putting physical and information security of command and control infrastructure in place (e.g., protecting from mishaps such as severed cables of ground stations during off-site building works, damage or wear of critical equipment through climatic conditions, or compromised mission control software).

## Trading Off Resilience and Capability in Architecture

Resilience has been included as a key criterion in the evaluation of alternative space architectures (National Security Space Strategy 2011) and ought to be taken into account at the beginning of the systems planning process as a “critical component to

define at system level” (OSD 2015, here 8). Aside from weighing the different elements of resilience against each other, also resilience itself must be traded off with other characteristics of a capability – indeed, since resilience is not understood as a capability itself, resilience and capability must be treated as distinct concepts (Jakhu and Pelton 2017, here 296).

Since in view of resource constraints the benefits of architectural resilience come at a cost, affordability is a key driver in this capability-resilience trade-off (cf. Pawlikowski et al. 2012, here 47). Implementing elements such as distribution or diversification means that other performance aspects of a system or architecture – e.g., sensor coverage, integration times, and procurement cost – may be constrained. These dependencies must be traded against their benefits across the system life cycle and the complete system hierarchy with regard to different threat scenarios (Aero-space 2018).

For want of extensive dedicated metrics, five tentative criteria to assess resilience of a functional architecture include the anticipated level of adversity, functional capability goals of the architecture itself, the risks of not achieving these goals in view of adversities, the severity of functional shortfall, and the duration of downtime that can be tolerated by the mission (DOD 2011).

---

## **Resilient Operations and Organizations: The High Reliability and Resilience Engineering Perspective**

Once hardware on the ground or in space has been commissioned, changes and modifications to increase the quality of resilience are either infeasible or involve considerable resources. Other system elements are, however, more malleable and may be actively adapted across the life cycle to different extent, including human operators, procedures, or mission rules (McLeod et al. 2016). Next to mission assurance for architecture, a second perspective on resilience hence focuses on operations and organizations rather than infrastructure. Rather than property of a system, resilience here means a continuous pursuit or process, not a characteristic that can be instilled in a system, rather, something that a system is enabled to *perform*.

Normal accident theory (NAT) posits that failure of complex sociotechnical systems in high-risk domains such as space is both inevitable and rare (Perrow 2007). In response to NAT, two proactive fields have formed in safety management across the past decades: high reliability organizing (HRO) and resilience engineering (Haavik et al. 2016). They propose that in view of inherently unsafe systems – or systems exposed to continuous risk – it is in fact the performance of human operators that contributes to safety under varying conditions (Dekker 2012). As they share fundamental terminology with the field of RAMS (Reliability, Availability, Maintainability, Safety) and dependability, and specifically include use cases in both civil and military domains, resilience engineering and high reliability organizing offer an important contemporary lens on aspect of resilience and its context that have not yet matured for the space domain in the mission assurance context.

## Resilience Through Sensemaking

Sectors and organizations that are understood through the HRO lens or operate according to HRO principles (i.e., air traffic management, aircraft carriers, utility grids) share fundamental characteristics with space systems. They are highly complex on all levels of the system hierarchy – respectively, nested into systems of systems – with interdependent elements, components, and parts that are tightly coupled and integrated and feature nonlinear interactions. In view of the constraints in the operational environment, they are governed by a high degree of causality, i.e., the laws of physics more so than purely organizational intent, and predominantly face either a physically hostile operating domain (i.e., submarine) or the handling and control of highly hazardous assets or processes (i.e., nuclear power plant). In operations, they rely on the collaboration of distributed actors that may be situated at a distance from the process in a control room environment; in several instances, the system in operation is either highly bespoke or of international significance and sophistication (i.e., a fusion experiment, sample return mission). (In comparison, automotive manufacturing and healthcare environments are also understood as complex undertakings and require a high degree of reliability and continuity but are characterized less by the constraints of physical causality, i.e., when processes come to a halt through a disturbance, the system does not necessarily fail (despite the cost incurred). In contrast, processes in domains such as nuclear power or missile operations require immediate attention and intervention both in routine operations and in view of anomalies in order to avoid irreparable damage or loss.)

Yet, despite tightly coupled processes and constant hazard, highly reliable organizations are able to maintain “continuously safe operations” (Weick and Sutcliffe 2001, here 9). To this end, HROs employ the principle of “collective mindfulness” (ibid., here 9–14). This describes an awareness of ongoing processes by all organizational constituents, combined with an acute understanding of the dependencies and implications of an individual operation or element. Specifically, and in contrast to other types of organizations, HROs operate according to five concrete principles:

- *Preoccupation with failure*, i.e., they cultivate an awareness of small lapses, disturbances, and weak signals; they encourage error reporting and analysis of near misses and foster a culture that challenges complacency and hubris in view of past success.
- *Reluctance to simplify interpretations*, i.e., they deliberately strive for nuanced pictures of a situation and do not rely purely on key indicators; they challenge received wisdom and hear diverse viewpoints.
- *Sensitivity to operations*, i.e., they maintain a situational picture of the “sharp end” (or front line) of operations, which allows continuous adjustments to be made in order to cope with external disturbances.
- *Deference to expertise*, i.e., they foster diverse thinking and an encouragement for decision-making beyond rigid hierarchies by those that are best placed to judge a situation based on their command of the subject matter rather than status or rank.



- *Commitment to resilience*, i.e., maintaining dynamic capabilities for recovery and containment of situations, including flexibility and creative solutions for unexpected problems, but also ensuring continuous supply of fresh resources (i.e., shift personnel) during a crisis or incident.

The final principle can be further understood through the field of resilience engineering. In extending the vantage point and analytical repertoire of HRO, particularly with regard to sensemaking of past, ongoing, and future events, Resilience engineering specifically places emphasis on operator interaction with, and as part of, a system (Leveson 2011; Hollnagel et al. 2008).

Similar to HRO, resilience engineering seeks to understand and leverage the significant part of operations where and how in the face of disturbance the system manages to remain available or “bounces back.” (Cf., when looking at a reliability metric of, e.g., 98% in traditional safety management approaches, focus would be directed not only at understanding the 2% of failure cases or incidents, i.e., through failure mode or error analysis, but on the considerable amount of time where “things go right” either in routine or during recovery of anomalies.) Organizational resilience is hence described as the “capability to recognize the boundaries of safe operations . . . to steer back from them in a controlled manner” (Dekker 2005) and as the “ability to anticipate and adapt to potential for surprise and error” (Reason 2008, here 8).

Practically, four key abilities contribute to this adaptation and control, i.e., the overall ability of predicting, planning, and executing (Hollnagel et al. 2008):

- *Factual*, learning from past experience such as incidents in view of devising practical measures to address resilience, knowing what has happened
- *Actual*, responding to actual disturbances and regular and irregular threats, i.e., know what to do, being capable of doing it
- *Critical*, monitoring the system’s own performance in order to respond to critical events, i.e., know what to look for and direct attention to the right areas
- *Potential*, anticipating potential disruptions, pressures, and their consequences in the near future, finding out and knowing what to expect

This collective “anticipation of the potential” is a key feature of resilient organizations (Hollnagel et al. 2006). Anticipation focuses on both past and future manifestations and pathways toward failure (Dekker 2012) and aims to make sense of events (i.e., incidents, successful operations). Crucially, it also involves investing resources in the anticipation, adaptation, and growth in response to disruption – both in view of negative stressors and novelty (Reason 2008). The latter part of “growth” represents a critical distinction to other assurance concepts: resilience engineering explicitly includes the possibility that a system is strengthened through meaningfully responding to a continuous barrage of internal and external disturbances. While this potential is usually not formally foreseen in systems planning (e.g., as a performance indicator) and its assessment is not afforded by current safety management tools, in space operations it has been anecdotally evident and crucial to functioning in routine or contingency operations (i.e., creating automated protocols to work around

frequently occurring ground station time constraints or outperforming nominal mission life time by ingeniously handling the fuel budget of a spacecraft) or even been assumed as an underlying necessity for missions with high degrees of uncertainty (i.e., devising cutting edge trajectories “on the fly” in response to gradual discovery of targets during special missions).

## Resilience Through Performance Variability

Personnel contribute to this quality of adaptation on organizational, team, and individual levels. Practically, they create resilience by adjusting their tasks, inserting buffers or automated routines, using heuristics and double checks, or devising decision-making aids (Dekker 2005, here 12–13) whenever the demands of a situation eclipse predefined rules in an otherwise highly proceduralized domain. This habitual or intentional adjustment is called “performance variability” (Hollnagel et al. 2008).

Rather than being understood as deviation from the norm (i.e., violation of a procedure), performance variability is “normal and necessary” and can be identified by determining the discrepancy of normative and descriptive models of work (ibid.). In space operations, the normative – or designer’s – model is described in mission rules, system specifications, formal training manuals, or flight plans as aggregate of procedures. The operator’s or “actual” model, however, incorporates also experience after commissioning, as operators “continually test their model against reality,” often under time and productivity pressures (Leveson 2011, here 42). Operators may thus determine the change or evolution of the system and its state and the need for subsequent updating of their mental model through varying their performance. These practices require what is termed efficiency-thoroughness trade-off, i.e., where operations have to be compromised in view of resource constraints and increasing demands (Hollnagel et al. 2008).

## Practical Measures

Specifically for space operations, some work has explored practical measures for resilience, for both the defense and civilian contexts, by transferring practice from external safety-critical sectors (McLeod et al. 2016; Peldszus 2015). These measures include activities and processes that can be implemented or integrated seamlessly in running operations or carry a comparatively modest cost when juxtaposed with changes in infrastructure, such as:

- *Operational simulation and exercises* using different degrees of fidelity for routine, contingency, and special operations
- *Human performance training* (i.e., communication, situation awareness skills for critical operations)
- *Actionable information and appropriate decision aids*, capturing of shared mental models (i.e., subsystems of an asset)
- Structured, standardized *anomaly resolution* (i.e., according to predefined protocols)

- Centralized, non-punitive *anomaly and near-miss reporting*
- Centralized *operational practice reporting* (incl. recovery and what went “well” in routine)
- Encouraging *smart tacit practice* (i.e., double checks, four-eye principle, informal communication)
- Fostering *culture of openness*, ensuring *availability of resources* to handle serious events
- Building in *slack* or backup plans in processes (including shift planning)

Implementing these measures can be achieved on a spectrum of resource intensity, from updating a rule or procedure, scheduling a short regular review forum, or distributing a familiarization resource to assigning a new position, commissioning a software tool, or rolling out a training campaign. Incentivizing the use of these measures, however, requires an organizational and operational culture that regards resilience as priority (McLeod et al. 2016) and recognizes the critical role of human operators in maintaining resilient operations.

## Assessing Resilience in Operations and Organizations

Whether the prerequisites for resilient performance are in fact in place can be evaluated by verifying the deployment and implementation of measures such as those highlighted above. However, whether a complex system really behaves in a resilient manner may arguably only be assessed through a case-by-case appraisal of concrete responses, in view of a specific threat and the particular state of the system at a given time (Haimes 2009). Describing and understanding the functioning of complex systems in routine and contingency may necessitate formal modeling techniques. (These would, for instance, be utilized for architectural trade-offs, cf. previous section.) In order to evaluate resilience, there are, however, additional approaches that include natural language and visual tools.

A structured evaluation of whether and how resilience measures are actually implemented can be performed through methods such as the resilience analysis grid. The method diversifies, in fine granularity, the four key abilities of organizations described earlier (factual, actual, critical, potential) and their requisite resources and processes. As to how far these measures then impact on operations – and are successful – can be analyzed through modeling methods such as the functional resonance analysis method, which considers the specific conditions, resources, input, and resulting states and can be applied in various operational domains and at various levels of a system.

---

## Disciplines Contributing to Resilience

In addition to the specific measures taken in design and operations to achieve resilience in the mission assurance and reliability context, there are a range of stand-alone fields that contribute to resilience in their own right (see Table 1).

**Table 1** High-level elements of resilience in the space domain at a glance

Mission assurance and deterrence	Resilience engineering	High reliability organizing	Contributing disciplines
Disaggregation Distribution Diversification Deception Proliferation Protection	Learning from factual Responding to actual Monitoring critical Anticipating potential	Preoccupation with failure Reluctance to simplify Sensitivity to operation Deference to expertise Commitment to resilience	Space situational awareness Partnerships Information sharing Foresight Transparency and confidence building measures
<i>Architecture</i>	<i>Operations</i>	<i>Organization</i>	<i>Governance</i>

## Resilience Through Space Situational Awareness

A key element to remaining resilient from a systems and operational perspective is the ability to understand and act upon risks in the orbital environment in real or near real time through Space Situational Awareness (SSA) (Pellegrino and Stang 2016, here 9). By producing actionable information on the location and behavior of space objects and natural hazards through a general recognized space picture and related services (e.g., collision avoidance), SSA constitutes a fundamental background function that enables the protection of critical services such as navigation and Earth observations. Furthermore, both in the operational and deterrence context, SSA is a prerequisite for resolving certain types of anomalies and for verifying activities that occur in the vicinity of a spacecraft (i.e., rendezvous and proximity operations). Finally, as one of the approaches to mitigating the proliferation of space debris, SSA links directly to the effort of resilience and sustainability of the various orbital regimes per se (McCormick 2013).

A comprehensive understanding of the overall operational environment through SSA benefits considerably from burden sharing. In its reliance on distributed sensor networks for surveillance and tracking, SSA is today viewed as a global undertaking. Efforts to share and fuse information and data from various different sources are currently gaining momentum.

## Resilience Through Transparency Measures and Partnerships

The growing heterogeneity and granularity of actors in the space domain both lend itself to – and indeed necessitates – cooperation and transparency. For recovery in operation but also to achieve redundancy already during architectural development, information sharing and cooperation constitute essential means (Jakhu and Pelton 2017, here 269). Resilience considerations specifically encompass the strategic engagement in partnerships with stakeholders in international and domestic government agencies, industry, and academia (Defense Science Board 2017). Allied or

partner systems are the subjects of protection efforts, but the forging of closer architectural, operational, and diplomatic ties with allies and partner also constitutes a key resilience measure as such (DOD 2012, here 14). Leveraging a wide range of capabilities facilitates directly the resilience concepts of diversification and distribution (i.e., through payloads hosted on allied or commercial platforms).

## Resilience Through Foresight

Enlarging the scale from operational anticipation that is characteristic of highly reliable and resilient enterprises, resilience must build on foresight in order to anticipate wider ranging future challenges (Pawlikowski et al. 2012). Foresight methods are used to explore uncertainties and chart various possible futures (Healey and Hodgkinson 2008). For resilience in space operations, they may range from the systematic cross-disciplinary scanning of risks, developments, and change drivers to the appraisal of low-probability-high-impact events (cf. rare but inevitable failure in normal accident theory) and the crafting of possible scenarios, to the in-depth exploration of specific potential event and the rehearsing of protocols in large-scale tabletop exercises and red teaming (Peldszus 2018). These activities are most frequently undertaken in collaboration with different actors and are employed to inform both operations and strategy. They thus contribute to the facilitation of collaborative decision-making and good governance for space as a resilient domain and global commons.

---

## Conclusion

Despite the current lack of globally shared nomenclature, two salient perspectives have emerged for the principles and practice of resilience for the space domain. They focus on maximizing the continuation and reliability of operations in various conditions or seek to imbue an architecture with qualities that minimize incentives for adversary actions in an evolving threat environment.

Resilience is likely to continue to feature as a key concept in space policy and systems planning. Straddling the fields of space security and reliability, it may inform, enrich, or even galvanize the more traditional security and safety management disciplines. Its incorporation in European policy may, on the one hand, be influenced by US thinking and its current narrow but very applicable focus; on the other hand, the assurance and deterrence context will be enriched by wider use of complementary insights from the civilian domain.

Quite certainly, the onset of the deployment of unprecedentedly large constellations will both exacerbate the dynamics of the operational environment of orbit and offer new challenges and avenues for the notion of resilience. Its apparent ubiquity and perseverance call for deepened engagement in further developing the nascent field. Specifically, there is a need for the cultivation of a broad discourse to facilitate shared nomenclatures, detailed taxonomies, and the development of assessment

methods. Here, much insight can be drawn from other high reliability domains: the scholarly and industrial communities of practice hailing from the nuclear, transport, and offshore sectors have been prolific – if not conclusive – in their quest for shared theory and application on resilience. Finally, it will be crucial to examine how notions of resilience are interpreted and addressed in the programs and strategies of other major spacefaring actors (Russia, China, India), whose advanced capabilities may be viewed in the context of both deterrence and high reliability.

---

## References

- A New Space Strategy for Canada (2019) Ministry of Innovation, Science and Economic Development, Alberta
- Aerospace (2018) Resilience for space systems: concepts, tools and approaches (ATR-2017-02226). Aerospace Corporation, Washington, DC
- Air Force Space Command (2016) Resiliency and disaggregated space architectures: a white paper. US Air Force, Colorado Springs
- Arnold DC, Hays PL (2013) Strategy and the security space enterprise. In: Sadeh E (ed) (2012) Space strategy in the 21st century: theory and policy. Routledge, London, pp 120–158
- Bendiek A (2017) A paradigm shift in the EU's common foreign and security policy: from transformation to resilience. German Institute for International and Security Affairs, Berlin
- BMVg (2016) Weissbuch zur Sicherheitspolitik und Zukunft der Bundeswehr. German Federal Ministry of Defence, Berlin
- Defense Science Board (2017) Task Force on Defense Strategies for Ensuring the Resilience of National Space Capabilities, March 2017, Office of the Secretary of Defense for Acquisition, Technology and Logistics, Washington D.C.
- Dekker S (2005) Ten questions about human error: a new view of human factors and system safety. CRC Press, New York
- Dekker S (2012) Just culture: balancing safety and accountability, 2nd edn. Ashgate, Burlington
- DOD (2011) Fact sheet: resilience of space capabilities. US Department of Defense, Washington, DC
- DOD (2012) Directive 3100.10: space policy (update 2016). US Department of Defense, Washington, DC
- ESPI (2018) Security in outer space: rising stakes in Europe. European Space Policy Institute, Vienna
- European Commission (2016) A space strategy for Europe, COM (2016) 705. European Commission, Brussels
- Haavik TK, Antonsen S, Rosness R, Hale A (2016) HRO and RE: a pragmatic perspective. *Saf Sci*. <https://doi.org/10.1016/j.ssci.2016.08.010>
- Haines YY (2009) On the definition of resilience in systems. *Risk Anal* 29(4):498–501
- Healey MP, Hodgkinson GP (2008) Troubling futures: scenarios and scenario planning for organizational decision making. In: Hodgkinson GP, Starbuck WH (eds) *The Oxford handbook of organizational decision making*. Oxford University Press, Oxford, pp 565–585
- Hollnagel E, Woods DD, Leveson NG (2006) Resilience engineering: concepts and precepts. Ashgate, Burlington
- Hollnagel E, Nemeth CP, Dekker S (eds) (2008) Remaining sensitive to the possibility of failure. Resilience engineering perspectives, vol 1. Ashgate, Burlington
- Jakhu RS, Pelton JN (2017) Global space governance: an international study. Springer, New York
- Johnson-Freese J (2016) Space warfare in the 21st century: arming the heavens. Routledge, New York
- Leveson NG (2011) Engineering a safer world: systems thinking applied to safety. MIT Press, Cambridge, MA

- McCormick PK (2013) Space debris: conjunction opportunities and opportunities for international cooperation. *Sci Public Policy* 40(6):801–813
- McLeod G, Nacouzi G, Dreyer P, Eisman M, Hura M, Langeland KS, Manheim D (2016) Enhancing space resilience through non-material means. RAND Corporation, Santa Monica
- Ministère des Armées (2019) Stratégie Spatiale de Défense: Rapport du groupe de travail « Espace », Ministère des Armées, Paris
- NSSS (2011) National security space strategy: unclassified summary. US Department of Defense and Office of the Director of National Intelligence, Washington, DC
- OSD (2015) Space domain mission assurance: a resilience taxonomy. Office of the Assistance Secretary of Defense for Homeland Defense & Global Security, Washington, DC
- Pace S (2015) Security in space. *Space Policy* 33(2):51–55
- Parly F (2018) Intervention de Florence Parly, ministre des Armées: Espace et défense, 7 September 2018, CNES, Toulouse. <https://www.defense.gouv.fr/actualites/articles/direct-florence-parly-s-exprime-sur-les-enjeux-de-l-espace-pour-la-defense>. Accessed 22 Jan 2018
- Pawlikowski E, Loverro D, Cristler T (2012) Space: disruptive challenges, new opportunities and new strategies. *Strateg Stud Q* 6(1):27–54
- Peldszus R (2015) The Human Element and System Resilience at the European Space Operations Centre, AMCO-TN-0006 and AMCO-TN-00011 (Internal Reports), ESOC, Darmstadt
- Peldszus R (2018) Foresight methods for multilateral collaboration in space situational awareness (SSA) policy and operations. *J Space Saf Eng* 5(2):115–120
- Pellegrino M, Stang G (2016) Space security for Europe. EUISS report no. 29, July 2016. EU Institute for Security Studies, Paris
- Perrow C (2007) *The next catastrophe: reducing our vulnerabilities to natural, industrial, and terrorist disasters*. Princeton University Press, Princeton/Oxford
- Prior T (2017) NATO: pushing the boundaries for resilience. CSS analyses in security policy, CSS report no. 213. Center for Security Studies, Zurich
- Reason J (2008) *The human contribution: unsafe acts, accidents and heroic recoveries*. Ashgate, Farnham
- Robinson J, Šmuclová M, Degl’Innocenti L, Perrichon L, Pražák J (2018) Europe’s preparedness to respond to space hybrid operations. PSSI report July 2018. Prague Security Studies Institute, Prague
- UK National Space Policy (2015) HM Government, London
- UK Space Security Policy (2014) HM Government, London
- US National Space Policy (2010) Office of the President of the United States, Washington, DC
- Weick KE, Sutcliffe KM (2001) *Managing the unexpected: assuring high performance in an age of complexity*. Wiley, New York



# Space Security Cooperation: Changing Dynamics

# 9

Jessica L. West

## Contents

Introduction .....	146
The Case for Cooperative Approaches to Space Security .....	146
Moderating Strategic Rivalry: Technical and Utilitarian Modes of Cooperation .....	148
From Practical to Symbolic: Cooperation in Space Exploration .....	149
Expanding Access to Space: Cooperation and Capacity-Building .....	151
Cooperation for Safety and Sustainability .....	153
New Patterns of Cooperation: Space Security Versus National Security .....	155
New Issues: The Moon and Space Resources .....	158
Conclusion: The Future of Space Security Cooperation .....	159
References .....	160

## Abstract

The security of outer space is a cooperative endeavor to achieve a shared benefit. Yet, while cooperation is essential for space security, it is often fraught. This chapter examines the logic for cooperation as an approach to space security, including supportive governance mechanisms, and traces the impetus and evolution of such efforts over time, marked by struggle to overcome strategic competition. Increasingly, competition is giving way to new patterns of cooperation focused on military alliances and new strategic interests. In this context, it is not clear that cooperation will be maintained as a core value and principle of space activities.

---

J. L. West (✉)  
Project Ploughshares, Waterloo, ON, Canada  
e-mail: [jwest@ploughshares.ca](mailto:jwest@ploughshares.ca)



## Introduction

The security of outer space is focused on the security and sustainability of outer space as a global environment that can be used safely by all, rather than the narrow interests of individual actors. At heart, this is a cooperative endeavor to achieve a shared benefit. Yet, while cooperation is both an individual and collective interest, it is rarely straightforward. Like geopolitical relationships on Earth, outer space is subject to not only cooperative impulses, but also competition, self-interest, power disparities, and fear. Sustaining the security of the outer space environment thus involves extensive coordination, but like a dance, it is also marked by missteps.

This chapter begins by examining the logic for international cooperation as an approach to space security, including supportive governance mechanisms. It then traces the impetus and evolution of cooperative efforts in outer space from technical coordination at the dawn of the space age, through large-scale exploration efforts symbolized by the International Space Station (ISS), capacity-building, and contemporary governance initiatives aimed at safety and sustainability. It is clear that international cooperation is a core value and pursuit of national space activities, and over time it has both widened and deepened. Yet, cooperation is at times stymied by competing values, particularly concerns for national security in outer space, reflecting the ups and downs of broader geopolitical relations and tensions. But cooperation is not merely a reflection of politics. As a mode of governing the security of outer space, cooperative relationships and practices contribute to trust, transparency, and interdependencies capable of transcending political pressures elsewhere.

Space security cooperation has thus been marked by an ongoing struggle to overcome strategic competition. Recently, however, such competition is giving way to new patterns of cooperation. Focused on national security *in* outer space rather than the security *of* outer space, the expansion of military alliances and security partnerships into the space domain – increasingly viewed as one of warfare – raises questions about the strategic stability of the outer space environment and the implications for collective wellbeing in outer space. Looking forward, the chapter also considers how heightened geopolitical competition and shifting strategic interests in outer space might influence emerging activities in outer space including lunar and human space exploration and possible resource extraction.

Cooperation is an essential and persistent feature of activities in outer space and necessary to achieve the long-term security of the outer space environment. But such cooperation is also fraught, striving, and sometimes failing to overcome strategic competition. As the nature of this competition changes alongside new actors and ventures, the continued value placed on cooperation is at risk of diminishing.

## The Case for Cooperative Approaches to Space Security

The 1967 Outer Space Treaty recognizes the “common interest of all mankind in the progress of the exploration and use of outer space for peaceful purposes” (OST). But

like all global commons, the use of outer space is subject to competing – even conflicting – interests. The natural resources of outer space, such as radiofrequency and orbital positions are limited and shared. The environment is fragile and vulnerable to contamination from the accumulation of debris. Growing use of outer space means that it is becoming more congested, especially in popular orbits where, in the next five years alone, the number of satellites in low Earth orbit (LEO) could grow tenfold if proposals for large-scale constellations advance. As a shared environment, threats to safety, security, and sustainability – be they manmade contamination and interference, or natural hazards such as space weather – are mutually harmful.

Despite the declaration of outer space as a province of all mankind, it is also a place of inequality. Long a domain of the powerful, technology and cost barriers limit both access to and use of space and by extension, the tremendous benefits that it supports including remarkable tools for communication, navigation, and vast data collection enabled by Earth observation. And while threats within the space environment are indiscriminate, the ability to mitigate harm is not equally shared.

Outer space is also a place of strategic competition and tensions. Initially marked by existential competition for military, scientific, technological, and economic supremacy exemplified by the space race, today the strategic use of outer space has evolved into dependency and intense military vulnerability.

From a governance perspective, outer space is thus inherently vulnerable to numerous challenges including a tragedy of the commons, persistent inequality, and security dilemmas. It is a place of mutual interests, but also competition, suspicion, and fear.

The concept of space security is a response to these challenges. Defined here as the “secure, and sustainable access to and use of space, and freedom from space-based threats” (West 2019), this approach to space security promotes a secure and sustainable space environment to assure safe and responsible access to and use for all, as promoted in the 1967 Outer Space Treaty. Reflecting a collective approach to the security of – and in – a global commons, the security of outer space depends on international cooperation.

Along with peaceful purposes, such cooperation is the bedrock of the international governance framework for outer space. Institutionally, the United Nations Committee on the Peaceful Uses of Outer Space (UN COPUOS) is the focal point of cooperation. Spurred by the confluence of scientific and military interests in outer space alongside Cold War competition, the Committee was established in 1959 by UN Resolution 1472 (XIV) “International cooperation in the peaceful uses of outer space.” Core to its mandate is to facilitate information exchange related to outer space activities, and to promote and support international cooperation as a means to expand the peaceful use of outer space and to avoid extending national rivalries into this domain. Today, with 92 Member States and growing, it maintains a prominent role in the governance of outer space.

International cooperation is also a key principle of space activities enshrined in the 1967 Outer Space Treaty, which, in addition to the United Nations Charter, provides the fundamental basis for legal order in outer space. Specifically, Article III of the treaty mandates that states pursue outer space activities “. . . in the interest of

maintaining international peace and security and promoting international co-operation and understanding” (1967).

Cooperation in outer space is thus essential, mandated, but often fraught. Security in and of outer space, where threats and vulnerabilities are shared and individual actions have collective consequences, mean that there is clearly a mutual benefit to cooperation. But fostering this cooperation requires overcoming strategic rivalry, national security concerns, and competing interests. Efforts to navigate these tensions in pursuit of shared safety, security, and sustainability benefits in outer space have been ongoing since the early days of space activities, built largely on the basis of technical and utilitarian modes of cooperation.

### **Moderating Strategic Rivalry: Technical and Utilitarian Modes of Cooperation**

The first space age is synonymous with the existential competition of the space race. But even amid deep, strategic rivalry, there were efforts to temper competition with cooperative impulses. The promise of cooperation was held out by U.S. President John F. Kennedy in his inaugural address where he declared “Let both sides seek to invoke the wonders of science instead of its terrors. Together let us explore the stars” (1961). Concretely, following his landmark declaration that the United States would land a man on the Moon within the decade, Kennedy is reported to have reached out to the Soviet Union on several occasions to foster cooperation (Kay 1998). However, terror ultimately overwhelmed cooperation. At a time of heated nuclear confrontation, Soviet reciprocity was foregone in favor of focused attention to the negotiation of a nuclear test ban treaty; later it was stymied by Kennedy’s death.

Cooperation was nonetheless established on more technical areas. A 1962 agreement facilitated cooperation in the exchange of weather data and the launching of meteorological satellites, as well as efforts to map the geomagnetic field of Earth, and in the experimental relay of satellite communications (Sagdeev and Eisenhower 2008). Such functional approaches to cooperation in outer space remain a core feature today, having evolved into what are considered global utilities. This includes the sharing of meteorological and climate data, open access to and interoperability of civilian positioning, navigation and timing services, and the increasing public availability of Earth observation (EO) data.

This coordination and sharing of data and services has been formalized through organizations such as the International Committee on Global Navigation Satellite Systems (ICG) established in 2005 under the umbrella of the United Nations to facilitate compatibility, interoperability, and transparency between systems. The Coordination Group for Meteorological Satellites provides a forum for the exchange of technical information on geostationary and polar-orbiting meteorological satellite systems. Collected data is made available to the World Meteorological Organization, which distributes it to more than 3,000 weather-forecast outlets in 187 member states and 6 territories. Efforts to share and expand access to Earth observation data include the Committee on Earth Observation Satellites, which has 62 member agencies from

around the world that work to coordinate and harmonize civil EO programs and data exchange from 170 satellites. Similarly, there is an international effort to create a Global Earth Observation System of Systems (GEOSS) that includes government agencies, academia, and the private sector, to enhance the sharing and integration of EO data worldwide. States also cooperate extensively for the use of satellite data to support disaster response and search and rescue through programs such as the International Charter on Space and Major Disasters and the Cospas-Sarsat international satellite system for search and rescue.

Such cooperation contributes to space security by providing essential global services that not only enrich lives, but also save them. This is the primary way in which most people on Earth access and enjoy the benefits of outer space. And, like in the early days of the space age, it remains critical to fostering cooperative relationships and reciprocity across diverse space actors. Indeed, on this basis of narrow, technical cooperation, cooperative relationships in outer space have extended much further, encompassing space exploration as both a practical and symbolic endeavor bridging self-interest and shared goals.

### **From Practical to Symbolic: Cooperation in Space Exploration**

Exploration beyond Earth is at the heart of efforts to access outer space. And perhaps more so than any other activity, exploration bridges the enduring tension between national interest and collective aspiration in outer space. This was evident with the landing of the Apollo 11 mission on the Moon in 1969, which marked both a national achievement and an historic moment for all of humanity. The astronaut remains an enduring symbol of such unity. Taking their place among national icons, astronauts are also global figures, assigned a special status as “envoys of mankind in outer space” under the Article V of the Outer Space Treaty, which affords them the right for assistance, rescue, and return by all states.

Indeed, despite the competitive nature of space activities during the Cold War, the pursuit of space exploration gradually enabled a critical precedent of cooperation, starting with the 1975 Apollo-Soyuz Test Project. Marking the first ever international human spaceflight, the Test Project symbolized growing détente between the United States and Soviet Union; but it was also practical and self-interested. Involving a nine-day spaceflight during which an Apollo spacecraft carrying three American astronauts docked with a Russian Soyuz spacecraft with a crew of two, the mission allowed both parties to test the feasibility of international space rescue through compatible rendezvous and docking systems. Critically, the mission also demonstrated the viability of cooperation on more sensitive areas of technology which continued throughout the Cold War, namely through the exchange of scientific data related to ongoing space probes and robotic missions (Launius 2016). And it laid a foundation for the cooperative spirit that has been a hallmark of space exploration since the end of the Cold War.

In space, the end of the Cold War was marked by a 1992 agreement between the United States and Russia that led to astronaut exchanges and docking of NASA’s

Space Shuttle with the Russian Mir space station. This process led to the creation of the International Space Station (ISS), an enduring symbol of space cooperation for the last two decades. Estimated to cost \$150 billion to date, the ISS is the single largest, and most expensive space venture ever undertaken. Featuring a permanent human presence in outer space, it is made possible through collaboration among core partners, namely NASA in the United States, Roscosmos in Russia, the European Space Agency, the Japan Aerospace Exploration Agency (JAXA), and the Canadian Space Agency. In all, the ISS has received contributions from 15 states and hosted 236 astronauts from 18 different countries and counting (NASA 2019b).

From a space security perspective, such cooperation is critical to expanding access to outer space. Indeed, the significant expense and technical challenges associated with space exploration means that it is almost impossible without the pooling of financial resources and technical expertise, which in turn helps to expand both individual and collective capacity and participation in outer space. Cooperation on space cooperation marks a meeting of self-interest and shared achievement.

Space exploration reflects both the security of outer space and the international cooperation necessary to sustain it. It is also a means to this end. While the ups and downs of cooperative ventures are influenced by geopolitical and national security interests, over time such cooperation and shared interests in space has transcended these dynamics. Collaboration provides a critical mode of transparency and promotes a shared understanding of space activities. Mutual dependency in such a challenging environment builds trust in a field of activity that overlaps with strategic competition. Working and living together in outer space demands not only language training, but cultural understanding. Much like the iconic Earthrise image instills a sense of shared humanity, cooperation and co-existence in outer space introduces a shared vulnerability and mutual dependency.

Indeed, today the United States and Russia remain bound together on the ISS, mutually dependent on one another for access to and use of it. Since the retirement of the Space Shuttle, NASA has been dependent on Russia for access via Soyuz, while Russia depends on the United States for satellite communication. Although both parties strive to end such dependency, this entrenched cooperation has largely transcended geopolitical tensions on Earth, including political fallout related to recent interventions in Ukraine. Joint activities on the ISS have been largely exempt from rising hostilities and sanctions elsewhere.

Nonetheless, there are exceptions to the spirit of cooperative space exploration, most notably between the United States and China. China is not a member of the ISS and cooperation between the United States and China is extremely limited. This is largely a reflection of security concerns, which escalated following the Chinese anti-satellite (ASAT) demonstration that successfully destroyed one of its own ageing weather satellites in 2007. In 2011, the U.S. Congress adopted legislation barring any scientific activity between the United States and China involving either the National Aeronautics and Space Administration (NASA) or the White House Office of Science and Technology Policy (United States Congress 2012). However, American law does not ban private sector agreements with China, and in 2017 SpaceX carried the first experiment independently designed and fabricated in China to the

ISS. Further, a 2015 inaugural Civil Space Dialogue initiated tentative efforts to improve cooperation and transparency between the two states (U.S. Department of State 2015). This dialogue is tepid but ongoing, a testament to both the importance and challenges of cooperative relationships in a strategic environment.

More recently, cooperative efforts related to space exploration have been expanding beyond advanced spacefaring states to include emerging ones. Led by UN COPUOS, the 50th anniversary meeting of the first United Nations Conference on the Exploration and Peaceful Uses of Outer Space (UNISPACE+50) took place in June 2018. First among seven thematic priorities was to expand global partnerships on space exploration and innovation, specifically to “promote cooperation between spacefaring states and emerging space states,” so that exploration becomes “open and inclusive on a global scale” (UN Office of Outer Space Affairs (OOSA) 2017). Reinforcing this goal, China marked the occasion by inviting all members of UN COPUOS to participate in its upcoming Tiangong-3 space station and intends to train astronauts from developing countries. In this way, cooperation in space exploration is a means to bridge not only strategic divides in outer space, but also varying abilities to access outer space. Indeed, capacity-building to expand access to outer space is another core feature of space security cooperation.

## **Expanding Access to Space: Cooperation and Capacity-Building**

The central tenet of space security is the ability for all to be able to access and use space for peaceful purposes. Today, in addition to the European Space Agency (ESA), eight countries have direct access to space through national space launch capabilities; more than 70 operate national satellites (Union of Concerned Scientists 2019). International cooperation has been essential to this growth in access to space.

Like space exploration, some initiatives are international. For example, the KiboCUBE joint project between UNOOSA and the Japan Aerospace Exploration Agency (JAXA) makes use of Japan’s Kibo module on the ISS to launch CubeSats on behalf of educational and research institutions from developing countries. But most cooperation is bilateral. NASA currently has over 700 agreements with international organizations (NASA 2019a), China has 120 (Xinhua 2018). And the Indian Space Research Organisation (ISRO) cooperates with at least 50 states (ISRO 2017). The essential role of bilateral relationships in expanding national capabilities is evident using the example of the United Arab Emirates (UAE). Established in 2014, its national space agency signed more than 16 cooperative agreements with international space agencies within the first 3 years of operation. (Permanent Mission of the United Arab Emirates to the United Nations 2017). Cooperative endeavors include advanced capabilities such as space exploration and human spaceflight.

Regional cooperation is also a critical tool for increasing access to outer space and its benefits. It is most developed in Europe, where the European Space Agency (ESA) facilitates space activities among its 22 Member States. A similar approach is being

adopted in Africa, where progress on an African space strategy and African Space Agency is spurring greater cooperation. Likewise, in 2019 the Arab Space Coordination Group was initiated by the UAE and ten other countries (Algeria, Bahrain, Egypt, Jordan, Kuwait, Lebanon, Morocco, Oman, Saudi Arabia, and Sudan); its first collective project will be an Earth observation satellite used to monitor the environment and climate.

And yet regional cooperation also illustrates the enduring tensions between cooperation and strategic competition. This is clear in Asia, where two competing organizations foster cooperation: the Asia-Pacific Regional Space Agency Forum (APRSAF) and the Asia-Pacific Space Cooperation Organization (APSCO). The APRSAF was established by Japan in 1993; it currently includes participation by public and private entities from 40 countries. Modest achievements include the Sentinel Asia collaborate initiative to apply remote-sensing capabilities to support disaster management in the region. APSCO, established by China in 2005, includes Bangladesh, China, Iran, Mongolia, Pakistan, Peru, Thailand, and Turkey. Its activities have focused on training and data-sharing, disaster monitoring, and an Asia-Pacific Ground-Based Space Object Observation System (APOSOS) for monitoring objects in Earth orbit.

Indeed, security tensions and competition mean that cooperative efforts are rarely straightforward. The example of India's GSAT-9 communications satellite is a case in point. Described as a "gift" for the South Asian Association for Regional Cooperation (SAARC), Pakistan nonetheless opted out of participation (Set 2017). Likewise, the BRICS (Brazil, Russia, India, China, and South Africa) economic association, with its goal of decreasing dependency on the West, also provides a vehicle for space cooperation, but struggles with internal competition. Nonetheless, it has agreed to a first substantive project, namely the creation of a "virtual" remote sensing satellite constellation through a data-sharing system.

It is also clear that cooperative efforts can reinforce rather than transcend strategic interests. Although still taking shape, China's ambitious Belt and Road development and infrastructure initiative may be a case in point. Intended to integrate China into a network of global trade, the Belt and Road includes a Spatial Information Corridor to bring participants into China's space-based infrastructure services, including the BeiDou satellite navigation system, satellite communications, meteorology, remote sensing, and space-based broadband Internet service (Hui 2018). Including 65 national participants as of 2018, it is described as a cooperative initiative aimed at capacity-building and common development across members.

Some have questioned the long-term aims of such deep integration (Robinson 2019). More concretely, however, it speaks to the presence of underlying strategic undertones that can influence space security cooperation and capacity building. Specifically, Pakistan's participation in 2018 was expanded to include access to the BeiDou's military service (Abi-Habib 2018). Indeed, the persistence and even growth of national security uses – and corresponding geopolitical tensions – in outer space can impede other areas of cooperation related to safety and sustainability, which are needed to mitigate the challenges associated with more extensive uses of outer space.

## Cooperation for Safety and Sustainability

While indicative of space security, growing access to and use of space is not without challenges. In particular, the natural environment of outer space, while seemingly vast, is also fragile. As a global commons, it is open to everyone, and almost everything, from satellites to Tesla Roadsters, giant disco balls, and advertising. Most of what we put into space never returns, contaminating the environment for future use. To avoid a tragedy of the commons – and to enhance the safety of operations for everyone – cooperation is essential. And it is increasingly taking place. Indeed, it is noteworthy that the limited dialogue between the United States and China is focused largely on safety including “space and terrestrial weather; space debris and spaceflight safety; and the long-term sustainability of outer space activities” (U.S. Department of State 2016). But here too, there are limits, largely imposed by national security interests.

The mitigation of space debris is one of the most significant examples of cooperative efforts to enhance the security of outer space. The Inter-Agency Space Debris Coordination Committee (IADC) evolved from cooperation between NASA and ESA following the creation of a large debris cloud in low Earth orbit caused by an Ariane 1 second stage explosion in 1986. It now includes 13 of the leading civil space agencies from around the world, including Roscosmos and the China National Space Administration (CNSA). The Committee published the first set of international guidelines related to space debris mitigation, a version of which was adopted by the UN General Assembly in 2008 as “voluntary measures to which all space actors should comply” (UNOOSA 2010). While implementation is uneven, collective efforts to limit the production of new debris in orbit have significantly reduced the rate of debris accumulation and contributed to enhanced sustainability of the environment.

Cooperation on safety is another core contribution to space security, primarily through efforts to mitigate natural threats including Near Earth Objects (NEOs) and space weather. Depending on size, a NEO that enters Earth’s orbit can damage or destroy populated areas such as cities, or even the planet itself. Cooperation is emerging to mitigate this risk. In 2013 members of UN COPUOS created two international networks to coordinate detection, early warning, and future planetary defense measures: the International Asteroid Warning Network (IAWN), and the Space Mission Planning Advisory Group (SMPAG). The goal of each network is to ensure that all countries – including those with limited space capabilities – are aware of the threats – and to enable global warning, mitigation, and response processes. Space weather is another focus of safety cooperation. Space weather refers to changes in the space environment and geomagnetic storms that stem from flares and electromagnetic radiation emitted from the sun, which threatens security of objects both in outer space and on Earth by causing radiofrequency blackouts, orbital drag on satellites, and powerful power surges. In 2017 the expert group first convened by UN COPUOS in 2014 laid out a roadmap for greater international cooperation and information exchange on space weather events aimed at developing global modelling and forecasting capabilities (UN COPUOS 2017). Separately, the



World Meteorological Organization is wrapping up a 4-year plan that includes similar aims.

Key to these efforts is the role of UN COPUOS in coordinating cooperation for improved safety and sustainability. One of its most significant achievements in this regard is the identification of, and agreement to, a set of 21 voluntary guidelines for the long-term sustainability of outer space activities. Adopted by the Scientific and Technical Subcommittee in 2018 and referred to the UN General Assembly in 2019 along with a comprehensive preamble, the guidelines are indicative of the intersection of space security and cooperation. As stated in the preamble, they are “premised on the understanding that outer space should remain an operationally stable and safe environment that is maintained for peaceful purposes and open for exploration, use and international cooperation by current and future generations, in the interest of all countries. . . .” (UN COPUOS 2018). The aim of the guidelines is to assist both individual and collective mitigation of risks; moreover, the guidelines emphasize that international cooperation is *required* to implement and monitor their effectiveness and impact.

Adoption of these guidelines is significant. In addition to articulating the link between cooperation, safety, and sustainability, they lend further impetus to the efforts on which states are already pursuing cooperation, such as space weather and debris mitigation. However, there are clear omissions. Beyond noting that they should be compatible with the “defense or national security” interests of states, the guidelines exclude activities more closely related to these interests. This includes issues that involve dual-use capabilities such as active debris removal and advanced rendezvous and proximity operations, as well as issues that approach arms control, such as restraints on intentional interference or harm of satellites. Also absent is an effort to create a more global or inclusive approach to space situational awareness. This issue lends insight into the tension between the security of outer space as a global commons that requires cooperation, and national security interests that drive strategic competition.

Indeed, while debris mitigation has emerged as a focal point of international cooperation for the security of outer space, safety from debris – largely a function of space situational awareness (SSA) – reflects much more cartelized modes of cooperation. An extension of space surveillance, SSA refers to the ability to generate actionable knowledge from surveillance data in order to identify, track, and catalog objects in orbit. This focus on action means that it is a critical capability for both safety *and* security in outer space. And, because no single actor has an absolute capability to precisely monitor every object on orbit, SSA depends on cooperation. But despite its widespread utility, there is no global system for monitoring objects and activities in outer space. Neither is there a global system to manage space traffic and safety.

This does not mean that there is no cooperation; indeed, cooperation on SSA is extensive, but also selective, and largely military (Lal et al. 2018). The most prominent measures are supported by the United States. The U.S. Department of Defense, which has by far the most advanced capabilities through its Space Surveillance Network of global terrestrial and space-based telescopes. It shares significant

information on a public-platform, free of charge, through the [Spacetrack.org](https://www.spacetrack.org) website as part of the SSA Sharing Program run by the Combined Space Operations Center under the U.S. Strategic Command (USSTRATCOM). The U.S. Department of Defense also supports general space traffic management by providing conjunction warnings to other operators.

However deeper cooperation to share classified data that supports more advanced safety and security needs on orbit is restricted to bilateral agreements between USSTRATCOM and key allies and security partners. As of early 2019, these included agreements with 19 states (the Netherlands, Brazil, the United Kingdom, the Republic of Korea, France, Canada, Italy, Japan, Israel, Spain, Germany, Australia, Belgium, the United Arab Emirates, Norway, Denmark, Thailand, and New Zealand), in addition to ESA and the European Organization for the Exploitation of Meteorological Satellites, and more than 77 commercial space companies (US Strategic Command Public Affairs 2019).

Other actors are in turn developing their own, independent SSA capabilities. This includes European states, who are pooling national capabilities under a Space Surveillance and Tracking Support Framework. Russia and China also maintain extensive national capabilities, but do not widely share data; China is working narrowly with APSCO partners to develop the Ground-Based Space Object Observation Network. Several private companies also have commercial SSA capabilities and services. Such duplication would be beneficial to space security if data were pooled or otherwise used for verification and corroboration, but it is not. Instead, the persistent lack of *global* collaboration and cooperation on SSA and corresponding efforts to manage traffic in space reflects the ongoing difficulty of balancing the security of space as a common interest and national security concerns linked to the growing use of outer space.

## **New Patterns of Cooperation: Space Security Versus National Security**

The physical security of objects in outer space is a core element of space security, entwining the objectives of national security with common security interests. In addition to natural threats such as space weather or impacts from debris, physical harm to satellites can include intentional efforts to interfere with space systems. From a space security perspective, core challenges include not only how to protect individual systems from harm, but also how to maintain strategic stability and prevent escalation of conflict into the space environment. This is a key function and goal of early efforts to foster cooperative space exploration activities and remains a feature of the ISS. However, the ability to adopt cooperative approaches on strategic issues closely related to national security such as restrictions on the deployment of weapons or the use of force in outer space remains the most intractable challenge to the security of outer space.

To be sure, there are mutual interests in preventing the use of military force in outer space, including overwhelming dependency on space assets for national

security as well as the indiscriminate and long-lasting harm that violent conflict could inflict on the space environment. These concerns coalesced following the 2007 ASAT demonstration by China, which both threatened assured access to critical space systems in low Earth orbit and created the largest ever debris cloud in space. The event also marked a turning point in strategic relations in outer space from self-restraint to a simmering arms race.

The OST includes some provisions to prevent the worst of foreseeable conflict in outer space, including a ban on the orbiting of weapons of mass destruction and all military installments on the Moon. Other restrictions on armed conflict in outer space are scant, and mostly bilateral. Evidence of nascent protections for strategically sensitive satellites can be glimpsed in the Anti-Ballistic Missile Treaty, the Strategic Arms Limitation Talks, the Intermediate-Range Nuclear Forces Treaty, the Threshold Test Ban treaty, the Peaceful Nuclear Explosions Treaty, the Strategic Arms Reduction Treaty, the Conventional Forces in Europe Treaty, and the second Strategic Arms Reduction Treaty, which all included measures barring interference with “national technical means of verification,” widely understood to mean satellites used to monitor treaty compliance (Black 2008). Although narrowly applied and eventually abrogated, the Anti-Ballistic Missile Treaty involved a restriction against the placement of ballistic missile interceptors in outer space. To be sure, this era also coincided with rampant and sometimes outlandish development of anti-satellite weapons. But self-restraint avoided the operational deployment of such weapons. The general belief was that space is too important to risk becoming a domain of military conflict.

This tacit cooperation to maintain the strategic stability of the outer space environment has eroded. Beginning with the abrogation of the ABM treaty by the United States in 2002, and including renewed interest and demonstration of ASAT capabilities including by China in 2007, the United States in 2008, and India in 2019, as well as the revival of Soviet-era weapons systems by Russia, there is now a simmering arms race in outer space. Insecurity generated by these activities is exacerbated by new on-orbit capabilities such as advanced rendezvous and proximity operations. These capabilities can support a range of both legitimate and more nefarious activities in outer space, blurring safety and security issues.

Efforts to agree to additional arms control measures in the Conference on Disarmament have stalled for over 30 years. So have efforts to develop additional voluntary measures related to behavior in outer space – for example through a code of conduct. A cooperative approach to support additional transparency and confidence-building measures (TCBMs) has also eroded (West 2018). In place of a shared belief in the need to avoid armed conflict in outer space, and international cooperation to restrict it, a growing number of states including China, India, Russia, France, Japan, the United Kingdom, and the United States now see space as a likely domain of armed conflict in the near future. From a strategic perspective, this shift introduces significant vulnerabilities for national security because of dependency on space systems for almost all military and security operations. Ongoing military developments such as a new United States Space Force are symptomatic of this growing sense of insecurity.

Like SSA, this vulnerability is leading to new patterns of selective cooperation based on deepening military alliances and strategic partnerships. Most cooperation involves the sharing of space-based capabilities and data for terrestrial military purposes. Examples include the participation of Canada, the Netherlands, and the United Kingdom in the U.S. Advanced Extremely High Frequency (AEHF) satellite program, and the shared use of the U.S. Wideband Global Satcom communications service by Canada, Denmark, Luxembourg, the Netherlands, New Zealand, and Australia. But such cooperation is expanding to include more formal alliance structures based on defense interests in outer space. This includes cooperation within the Five Eyes intelligence alliance (Australia, Britain, Canada, New Zealand, and the United States) such as the sharing of signals intelligence. Five Eyes partners also participate in the annual U.S. Air Force Space Command Wargames (Schriever wargames) which in recent years has expanded to include France, Germany, and Japan. Expanded cooperation is the focus of the newly renamed Combined Space Operations Center, which provides command and control of space forces and features greater cooperation with U.S. allies and partners including the Five Eyes, Germany, and Japan. The NATO (North Atlantic Treaty Organization) alliance is also making moves to recognize space as a domain of warfare, and military cooperation.

The number of security partnerships in outer space is growing, particularly in Asia. The long-standing US–Japan alliance now firmly includes defense cooperation in space. The United States has also increased defense-related cooperation in space with India, now a major defense partner. Japan and India are also coordinating bilaterally; in 2018, the Japan–India Space Dialogue included a focus on security, namely sharing satellite data and surveillance technology (Hayashi 2018). India and France, which had long cooperated on civil space programs, have also extended cooperation to security applications (Rajagopalan 2018). Likewise, India and Vietnam have expanded their strategic relationship to include defense cooperation in space, primarily through satellite imagery (Parameswaram 2018). China’s ongoing cooperative endeavors also have strategic undertones, particularly the Belt and Road Initiative, which includes military cooperation with Pakistan and could expand to include additional partners.

There are positive aspects to such cooperation. The pursuit of objectives such as inter-operability and shared capabilities builds capacity and is a key mode of resilience in outer space: the ability to withstand interference with a satellite’s capabilities and maintain core functions. As a technical ability, resilience can enhance security to both deliberate and natural threats, bridging safety and security concerns in outer space. This has been a clear benefit of global cooperation related to satellite services for positioning, timing and navigation. Some argue that resilience could also deter aggression in space and stabilize the strategic environment (Air Force Space Command 2016). But the extension of strategic partnerships into space could also further escalate military tensions and even conflict in outer space, particularly in the absence of broader cooperative efforts to restrict the most damaging forms of conflict and protect strategic assets. This is particularly concerning in the face of rising geopolitical competition and acute vulnerability in outer space.

Further, it is also unclear how rising strategic competition and deep but narrow security cooperation in outer space will affect emerging areas of space activities such as lunar exploration and resource extraction.

## **New Issues: The Moon and Space Resources**

China's historic robotic landing on the far side of the Moon in 2019 heralded a new focus of human activity in outer space defined by lunar exploration and the possible exploitation of space-based resources. Other missions – either underway or planned – include India's Chandrayaan 2 robotic mission to the lunar South Pole and NASA's new Artemis program to build a lunar Gateway in orbit around the Moon and return American astronauts to the lunar surface. China has long-term plans to send astronauts to the Moon and develop a research base there. The European Space Agency also has a robotic lunar program and interest in resource extraction, as does Japan. The collective focus is on the lunar south pole, where resources critical for human survival and sources of power – including water ice and helium-3 – are known to exist. Unlike in the past, the goal is not merely to touch the Moon, but to leave a permanent mark: to establish bases and even human settlements, and to extract resources. Non-state actors are also participating. In 2019 SpaceIL launched the first private robotic lander to the Moon. Commercial ventures such as Moon Express – which focus on extracting the Moon's resources – are also set to arrive. Several companies are setting up businesses to shuttle items between Earth and the Moon. Billionaires Elon Musk (SpaceX) and Jeff Bezos (Blue Origin) aim to establish private exploration programs and human colonies. Whether or not individual missions advance, the long-term trend is toward a more expansive and possible exploitive human presence in outer space. Implications for the cooperative security of outer space are unclear.

Although colonization and the search for resources are long-standing themes of human history, they introduce new questions in relation to the security of outer space. These include issues related to contamination and the environmental integrity of the Moon; processes for – and the implications of – claiming locations for research and settlement; the mingling of scientific, commercial, and military interests; and how to extend the benefits of lunar access and extractive resources in space to the global community. Critically, these new activities reinforce established tensions between cooperation and strategic competition that drive dynamics related to sustainability, security, and equity in the global commons of outer space.

Thus far, signs of cooperation are strong. The return to the Moon is a global pursuit. The 2018 Global Exploration Roadmap published by the International Space Exploration Coordination Group describes “an emerging international consensus to proceed with lunar exploration using a cislunar platform as the initial step in space exploration beyond low Earth orbit” (International Space Exploration Coordination Group 2018). The Group of 15 space agencies, including NASA, Roscosmos, and CNSA, participate in this nonbinding initiative, discussing common interests and identifying potential areas of cooperation. It has also adopted new terms of reference as a basis to foster international space cooperation and dialogue. Other cooperative

initiatives include the nonprofit Moon Village Association, which is working to foster an international collaborative approach to lunar exploration and For All Moonkind, which seeks to protect and preserve human heritage including individual landing sites on the Moon.

There is also considerable bilateral cooperation emerging. Significantly, NASA received Congressional approval to collaborate with China on lunar landing research and transmitted images of the lunar landing site for the Chang'e 4 mission in 2019 (David 2019). China has invited additional international partnerships for its planned Chang'e 6 lunar sample return mission. The United States is engaging both international and private sector partners for the Artemis human exploration program. India and Japan are pursuing joint projects; China has also reached out to India.

Some efforts to cooperate on the governance of resource-use are taking shape. The Hague International Space Resources Governance Working Group is formulating governance recommendations and guidelines; the *Draft Building Blocks for the Development of an International Framework on Space Resource Activities* was published in 2017 (Universiteit Leiden 2017). There are discussions within UN COPUOS to potentially create a working group to further explore legal considerations. Bilaterally, Luxembourg – one of the greatest proponents of private sector resource extraction in outer space – is cooperating with like-minded countries including the UAE and Japan.

These are all good signs, but there are few agreed upon rules to put inspiration into practice. Efforts to operationalize peaceful uses and cooperative approaches of the OST in the 1979 Moon Agreement failed. And despite a global focus, the sense of a new race to the Moon and underlying strategic interests – including a possible scramble for resources – cannot be ignored. Beyond a focus on national security in outer space, the United States aims for pre-eminence in the space domain (The White House 2018), while China seeks to be a “space power in all respects” (The State Council Information Office of the People’s Republic of China 2016). Private and commercial interests introduce yet another competitive component. How these tensions will interact with lunar exploration – and resource ambitions – is not clear. Neither is it clear that the spirit of cooperation that informs the principles of peaceful and equitable use of outer space in the OST will endure. As U.S. Vice President Pence has asserted, those who get there first – and stay – will write the “rules and values of space” (The White House 2019). The future of cooperation in outer space may depend on who gets there first.

---

## **Conclusion: The Future of Space Security Cooperation**

Outer space is a fragile environment, a critical resource, and a focus of strategic competition. Maintaining the ability of this domain to support safe, sustainable, and secure access and use for all – the essence of space security – requires cooperation. Further, cooperation is embedded as a core value within the institutions and laws that govern outer space, a *raison d'être* of both the UN Committee on the Peaceful uses of Outer Space, and the Outer Space Treaty. Over time, cooperative efforts to

improve the safety and sustainability of space operations, and to expand global access to outer space, have widened, increasing both individual and collective capacity and well-being in a challenging environment.

But while cooperation is the norm in outer space, it is not straightforward. National security interests present the most persistent impediment. At times cooperation has provided a way to transcend relationships by developing trust and transparency. The ISS is a key example. Other times, cooperation trails strategic and geopolitical interests, marked most strongly by the ongoing absence of international cooperation to limit the use of force in outer space. Combined with intense dependency on vulnerable space-based systems for military and national security objectives, this void is giving way to new, narrow patterns of cooperation among national security allies and partners. While such cooperation can enhance security *in* space for those involved, it may come at cost to the long-term security *of* space by increasing strategic rivalry and facilitating the escalation of conflict into outer space.

New uses and users of outer space are also changing the dynamics of space security cooperation. Examining the revival of lunar and human exploration alongside interest in the exploitation of space-based resources indicates a shift toward a more intense, long-term, and strategic human activities in presence that will leave a fundamental mark on worlds beyond our planet. This shift is being undertaken with considerable international cooperation. And yet underlying strategic rivalry as well as commercial and private interests may well impede efforts to implement the values of the Outer Space Treaty, including peaceful uses, cooperation, and global benefit. A cooperative approach to the security of outer space remains a prudent way to ensure that these values are upheld.

---

## References

- Abi-Habib M (2018) China's 'Belt and Road' plan in Pakistan takes a military turn. *New York Times*, 19 December. <https://www.nytimes.com/2018/12/19/world/asia/pakistan-china-belt-road-military.html>. Accessed 11 Sept 2019
- Air Force Space Command (2016) Resiliency and disaggregated space architectures. White paper. <https://www.afspc.af.mil/Portals/3/documents/AFD-130821-034.pdf?ver=2016-04-14-154819-347>. Accessed 11 Sept 2019
- Black S (2008) No harmful interference with space objects: the key to confidence-building. In: *Security in space: the next generation*, United Nations Institute for Disarmament Research, 31 Mar–1 Apr
- David L (2019) Farside politics: The West eyes Moon cooperation with China. *Scientific American*, 7 February. <https://www.scientificamerican.com/article/farside-politics-the-west-eyes-moon-cooperation-with-china/>. Accessed 11 Sept 2019
- Hayashi S (2018) Japan-India 'Space-Dialogue' to include surveillance sharing. *Nikkei Asian Review*, 9 December 2018. <https://asia.nikkei.com/Politics/International-relations/Japan-India-Space-Dialogue-to-include-surveillance-sharing>. Accessed 11 Sept 2019
- Hui J (2018) The spatial information corridor contributes to UNISPACE+50. China National Space Administration technical presentation to the scientific and technical subcommittee of the UN Committee on the Peaceful Uses of Outer Space <http://www.unoosa.org/documents/pdf/copuos/stsc/2018/tech-08E.pdf>. Accessed 11 Sept 2019
- Indian Space Research Organization (ISRO) (2017) International cooperation. <https://www.isro.gov.in/international-cooperation>. Accessed 9 Sept 2019

- International Space Exploration Coordination Group (2018) Government representatives from 45 countries and international organisations meet at the 2nd International Space Exploration Forum (ISEF2), 26 April. <https://www.globalspaceexploration.org/wordpress/?p=792>. Accessed 11 Sept 2019
- Kay WD (1998) John F. Kennedy and the two faces of the U.S. space program, 1961–63. *Pres Stud Q* 28(3):573–586
- Kennedy JFK (1961) Inaugural address. Special message to Congress on Urgent National Needs, 25 May 1961, Washington, DC. John F. Kennedy Library and Museum website: <https://www.jfklibrary.org/asset-viewer/archives/JFKWHA/1961/JFKWHA-032/JFKWHA-032>
- Lal B et al (2018) Global trends in space situational awareness (SSA) and space traffic management (STM). Science and Technology Policy Institute, 10 October. [https://csis-prod.s3.amazonaws.com/s3fs-public/event/181010\\_SSA\\_CSIS.PDF](https://csis-prod.s3.amazonaws.com/s3fs-public/event/181010_SSA_CSIS.PDF). Accessed 11 Sept 2019
- Launius R (2016) Key developments in USA/USSR space cooperation during the Cold War. <https://launiusr.wordpress.com/2016/08/15/some-key-developments-in-usausrr-space-cooperation-during-the-cold-war/>. Accessed 9 Sept 2019
- NASA (2019a) Active international agreements by signature date (as of 30 June 2019). [https://www.nasa.gov/sites/default/files/atoms/files/house\\_approps\\_action\\_international\\_saas\\_active\\_as\\_of\\_6-30-2019.pdf](https://www.nasa.gov/sites/default/files/atoms/files/house_approps_action_international_saas_active_as_of_6-30-2019.pdf). Accessed 9 Sept 2019
- NASA (2019b) International cooperation. [https://www.nasa.gov/mission\\_pages/station/cooperation/index.html](https://www.nasa.gov/mission_pages/station/cooperation/index.html). Accessed 9 Sept 2019
- Parameswaram P (2018) India-Vietnam defense relations in the spotlight with bilateral visit. *The Diplomat*, 18 June. <https://thediplomat.com/2018/06/india-vietnam-defense-relations-in-the-spotlight-with-bilateral-visit/>. Accessed 11 Sept 2019
- Permanent Mission of the United Arab Emirates to the United Nations (2017) UAE statement to the fourth committee on international cooperation in the peaceful uses of outer space. 17 October. [https://www.un.int/uae/statements\\_speeches/uae-statement-fourth-committee-%E2%80%9CInternational-cooperation-peaceful-uses-outer](https://www.un.int/uae/statements_speeches/uae-statement-fourth-committee-%E2%80%9CInternational-cooperation-peaceful-uses-outer). Accessed 9 Sept 2019
- Rajagopalan RP (2018) From sea to space: India and France deepen security cooperation. *The Diplomat*, 15 March. <https://thediplomat.com/2018/03/from-sea-to-space-india-and-france-deepen-security-cooperation/>. Accessed 11 Sept 2019
- Robinson J (2019) State actor strategies in attracting space sector partnerships: Chinese and Russian economic and financial footprints. Prague Security Studies Institute. [http://www.pssi.cz/download/docs/6886\\_executive-summary.pdf](http://www.pssi.cz/download/docs/6886_executive-summary.pdf). Accessed 11 Sept 2019
- Sagdeev R, Eisenhower S (2008) United States-Soviet space cooperation during the Cold War. NASA. [https://www.nasa.gov/50th/50th\\_magazine/coldWarCoOp.html](https://www.nasa.gov/50th/50th_magazine/coldWarCoOp.html). Accessed 9 Sept 2019
- Set S (2017) India's regional diplomacy reaches outer space. *Carnegie India* [https://carnegieendowment.org/files/7-3-2017\\_Set\\_IndiaRegionalDiplomacy\\_Web.pdf](https://carnegieendowment.org/files/7-3-2017_Set_IndiaRegionalDiplomacy_Web.pdf). Accessed 11 Sept 2019
- The State Council Information Office of the People's Republic of China (2016) China's space activities in 2016. White Paper 27 December. <http://www.scio.gov.cn/wz/Document/1537091/1537091.htm>. Accessed 11 Sept 2019
- The White House (2018) President Donald J. Trump is unveiling an America first national space strategy. 23 March. <https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy/>. Accessed 11 Sept 2019
- The White House (2019) Remarks by Vice President Pence at the fifth meeting of the National Space Council, Huntsville Alabama, 26 March. <https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-fifth-meeting-national-space-council-huntsville-al/>. Accessed 11 Sept 2019
- Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies (Outer Space Treaty) (1967). <https://2009-2017.state.gov/t/isn/5181.htm>. Accessed 11 Sept 2019
- UN COPUOS (2017) Report of the scientific and technical subcommittee on its fifty-fourth session, held in Vienna from 30 January to 10 February 2017. [http://www.unoosa.org/oosa/oodoc/data/documents/2017/aac.105/aac.1051138\\_0.html](http://www.unoosa.org/oosa/oodoc/data/documents/2017/aac.105/aac.1051138_0.html). Accessed 11 Sept 2019
- UN COPUOS (2018) Guidelines for the long-term sustainability of outer space activities. Conference room paper by the Chair of the working group on the long-term sustainability of space



- activities (June). [http://www.unoosa.org/res/oosadoc/data/documents/2018/aac\\_1052018crp/aac\\_1052018crp\\_20\\_0\\_html/AC105\\_2018\\_CRP20E.pdf](http://www.unoosa.org/res/oosadoc/data/documents/2018/aac_1052018crp/aac_1052018crp_20_0_html/AC105_2018_CRP20E.pdf). Accessed 11 Sept 2019
- Union of Concerned Scientists (2019) Satellite database. <https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database>. Accessed 9 Sept 2019
- United States Congress (2012) H.R.2112 – consolidated and further continuing appropriations act. Sec. 539. <https://www.congress.gov/bill/112th-congress/house-bill/2112/text>. Accessed 9 Sept 2019
- United States Department of State (2015) The first meeting of the U.S.-China space dialogue. Media note. [www.state.gov/r/pa/prs/ps/2015/09/247394.htm](http://www.state.gov/r/pa/prs/ps/2015/09/247394.htm). Accessed 9 Sept 2019
- United States Department of State (2016) The second meeting of the U.S.-China space dialogue. Media note, October 24. <https://2009-2017.state.gov/r/pa/prs/ps/2016/10/263499.htm>. Accessed 11 Sept 2019
- Universiteit Leiden (2017) Draft building blocks for the development of an international framework on space resource activities, September. <https://www.universiteitleiden.nl/binaries/content/assets/rechtsgeleerdheid/instituut-voor-publiekrecht/lucht%2D%2Den-ruimterecht/space-resources/draft-building-blocks.pdf>. Accessed 11 Sept 2019
- UNOOSA (2010) Space debris mitigation guidelines of the committee on the peaceful uses of outer space. United Nations. [http://www.unoosa.org/pdf/publications/st\\_space\\_49E.pdf](http://www.unoosa.org/pdf/publications/st_space_49E.pdf). Accessed 11 Sept 2019
- UNOOSA (2017) UNISPACE +50 thematic priorities, p 3. [http://www.unoosa.org/documents/pdf/unispace/plus50/thematic\\_priorities\\_booklet.pdf](http://www.unoosa.org/documents/pdf/unispace/plus50/thematic_priorities_booklet.pdf). Accessed 9 Sept 2019
- US Strategic Command Public Affairs (2019) USSTRATCOM, Polish space agency sign agreement to share space services, data. USSTRATCOM, 11 April. <https://www.stratcom.mil/Media/News/News-Article-View/Article/1811729/usstratcom-polish-space-agency-sign-agreement-to-share-space-services-data/>. Accessed 11 Sept 2019
- West J (2018) Why the chances of conflict in outer space are going up. *Ploughshares Monit* 39(4), winter. [https://ploughshares.ca/pl\\_publications/why-the-chances-of-conflict-in-outer-space-are-going-up/](https://ploughshares.ca/pl_publications/why-the-chances-of-conflict-in-outer-space-are-going-up/). Accessed 11 Sept 2019
- West J (ed) (2019) *Space security 2019*. Project Ploughshares, Waterloo
- Xinhua (2018) China strengthens international space cooperation. *China Daily*, 19 April. <http://www.chinadaily.com.cn/a/201804/19/WS5ad899eea3105cdc6f5195a1.html>. Accessed 9 Sept 2019



# Strategic Competition for Space Partnerships and Markets

# 10

Jana Robinson, Tereza B. Kupková, and Patrik Martínek

## Contents

Introduction .....	164
Global Chinese and Russian Economic and Financial Space Activities .....	165
Africa .....	169
Latin America .....	169
Europe .....	171
The Arctic .....	173
Antarctica .....	174
The Middle East .....	175
South and Southeast Asia .....	175
Western, Central, and Eastern Asia .....	176
Top Space Sector Capture Trends .....	177
Key Findings .....	178
Conclusion .....	180
References .....	180

## Abstract

China and Russia's global space footprint in the economic and financial (E&F) domain is not well understood today. This chapter, through analyses of space-related transactions of China and Russia globally, describes the pro-active approach to international space partnerships by these two state actors. It concludes that these partnerships are often skewed, exposing recipient countries to

---

J. Robinson (✉)

Space Security Program, Prague Security Studies Institute (PSSI), Prague, Czech Republic  
e-mail: [jrobinson@pssi.cz](mailto:jrobinson@pssi.cz)

T. B. Kupková

Prague Security Studies Institute (PSSI), Prague, Czech Republic  
e-mail: [kupkova@pssi.cz](mailto:kupkova@pssi.cz)

P. Martínek

The Prague Security Studies Institute (PSSI), Prague, Czech Republic  
e-mail: [martinek@pssi.cz](mailto:martinek@pssi.cz)

vulnerabilities and dependencies on the benefactor(s). The more subtle strategy deployed in the developed, democratic countries to gain influence is conducted on an incremental basis (e.g., through commercial contracts, academic exchanges, scientific research). The other approach, described as “space sector capture,” mostly involves developing countries and consists of offering package deals of capabilities, services, and financing, creating source-supplier relationship and long-term dependencies. The chapter argues that the pace and nature of these international space partnerships concluded by China and Russia present a strategic and competitive challenge for Europe, the USA, and other allies, including the development of global space governance, as well as market based on transparency, good governance, and disclosure.

---

## Introduction

The actions and conduct of Russian and Chinese state-owned and -controlled enterprises (SOEs) are often driven by both commercial *and* strategic considerations. This has become increasingly evident with the emergence of new brands of soft power projection adopted by both countries. In the economic and financial (E&F) domain, this means seeking to gain influence and strategic advantage over targeted states via ostensibly commercial, legal transactions, and projects (e.g., acquisitions, partnerships, loans, joint ventures, minority investments).

There is a dearth of understanding concerning how China and Russia are using the legitimate E&F domain to compromise the integrity of the space sectors of various countries that lack space programs, adequate funding, operating personnel, and technical expertise. These include various levels of “space sector capture” achieved through the offer of end-to-end capabilities (i.e., vertically integrated packages of design/manufacturing of satellite(s), launch services/launch insurance, ground segment construction/equipment, provision of operating personnel, the training of local staff, and financial assistance) (Robinson et al. 2019).

These offers often involve the use of nonmarket trade and financial practices for the purpose of expanding their global space footprint at a strategic level (with a number of associated operational, political, geographic, and military benefits). This is being accomplished through securing desired foreign projects/assets, beachheads in priority regions, the acceptance of subsidized loans often to non-creditworthy state borrowers to acquire political leverage and/or secure the collateralized assets in default scenarios. China’s and Russia’s economic and financial activities in the developed, democratic countries involve more incremental approach, often through seemingly benign scientific research/development, academic exchanges, individual commercial contracts, or broader funding commitments beyond the space sector (Robinson 2018a).

As the economies of China and Russia are inextricably linked with their governments, its companies do not operate as traditional commercial enterprises. Many decisions pertaining to overseas investments are subject to approval by government authorities. State-controlled enterprises, including quasi-private companies, usually

have some level of state involvement in their management structures and are obliged to comply with government policies and directives.

The activities of these companies in the international trading and financial systems are designed to appear benign and commercial, providing space aspirants with capabilities they crave, ostensibly to advance the prosperity and security of these targeted countries. Countries lacking a space program, adequate funding, and technical expertise are generally open to such seemingly magnanimous offers, even if it means their countries could well become perilously dependent on these outside benefactors (Robinson 2018b).

Such international partnerships result in dependency, even control, over the space sectors of the recipient countries (e.g., Belarus, Bolivia, Nigeria, Pakistan, Sri Lanka, and Venezuela). The transactions, including offers of large-scale financing at below-market terms, are primarily for the purpose of expanding China and/or Russia's global space footprint at a strategic level (with a number of associated operational, political, geographic, and military benefits) (Robinson 2018c).

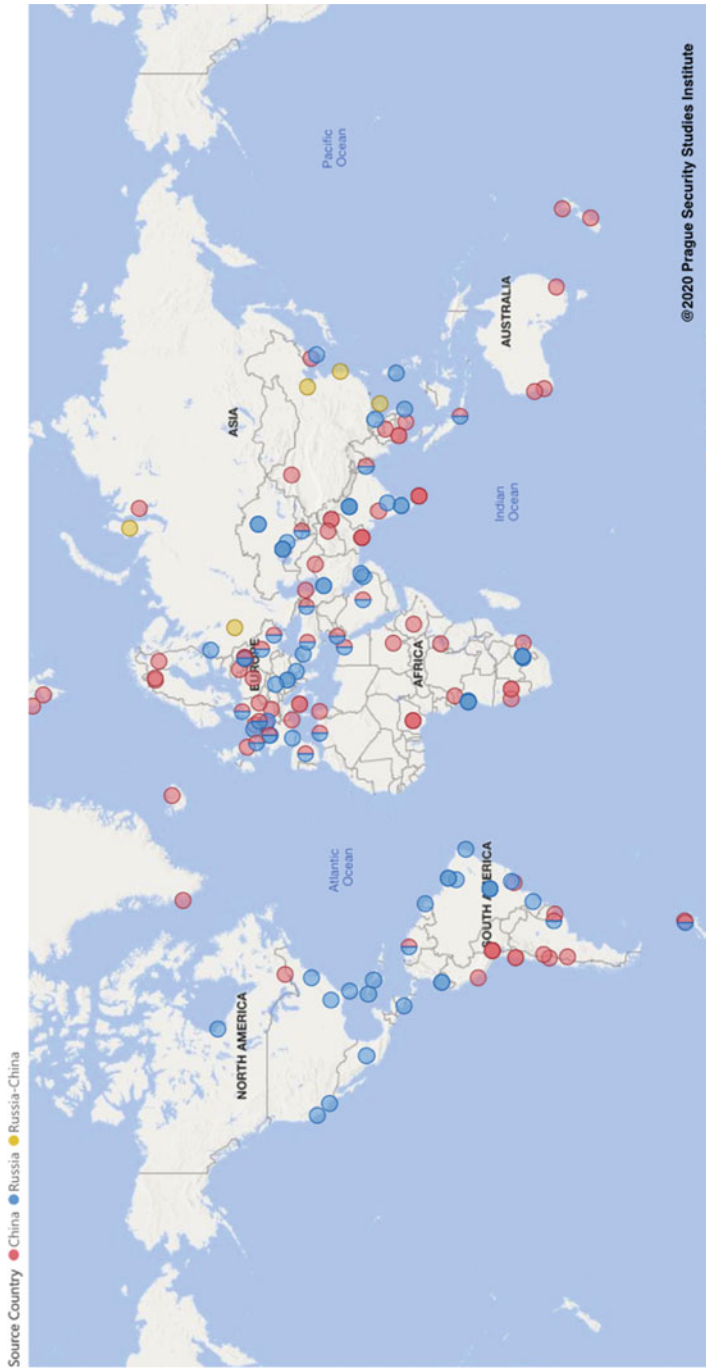
This article provides an overview concerning how China and Russia are using the legitimate E&F domain to compromise the integrity of the space sectors of various countries that lack space programs, adequate funding, operating personnel, and technical expertise. Through granular analysis of space-related transactions of Chinese and Russian state-controlled enterprises, the article demonstrates that this trend represents a material risks to the targeted countries from the perspectives of national security and sovereignty. In short, this chapter introduces a new risk category within the space security portfolio, namely the economic and financial (E&F) operations of nondemocratic state actors. It brings forward the above-referenced "space sector capture" concept and delineates its elements. It then describes the transactional approach of China and Russia to international space partnerships. Finally, it offers key findings and recommendations.

---

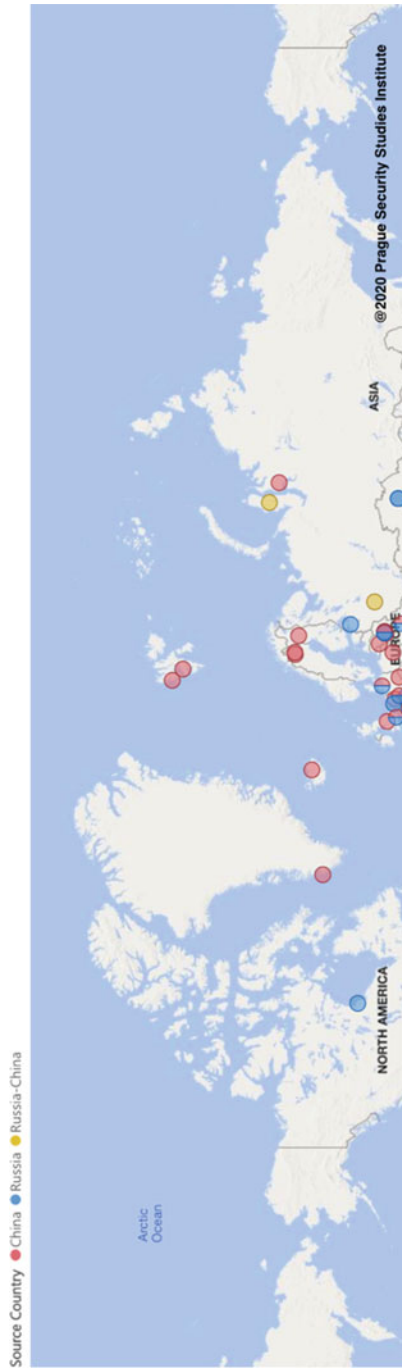
## **Global Chinese and Russian Economic and Financial Space Activities**

The analysis provided in this section draws from the research, including an open-source database, of the Prague Security Studies Institute (Robinson et al. 2019) concerning the strategic and commercial dimensions of space-related Chinese and Russian economic and financial activities globally. It provides an overview of prominent space-related partnering arrangements, which often involve partial or full dependency of the recipient countries on Chinese or Russian financing, technology, equipment, services, and/or expertise.

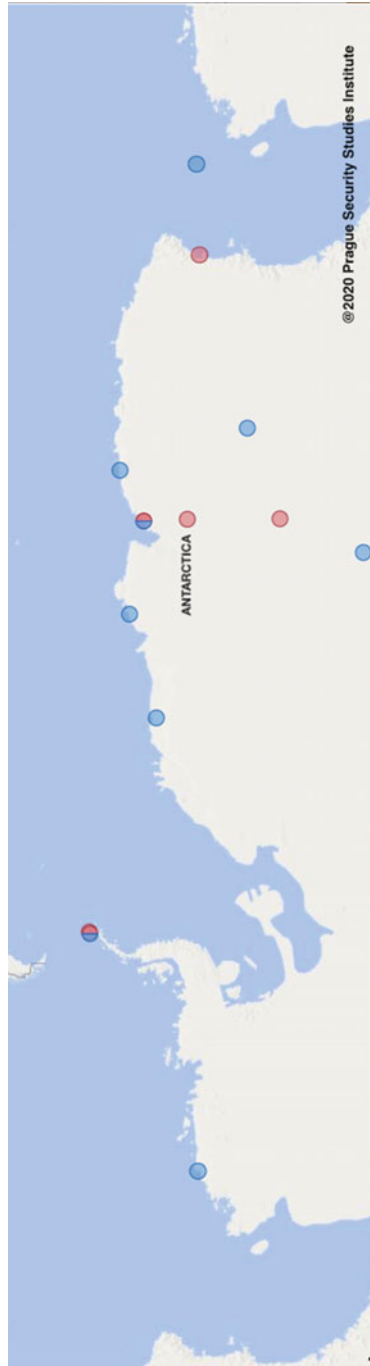
As of February 2020, China and Russia have been actively engaged in space partnerships in at least 78 countries (see Fig. 1). These two state actors have been especially active in Latin America, Europe, South/Southeast Asia, and Africa. China has also increased substantially its outreach to the Arctic countries in the past decade (Figs. 2 and 3).



**Fig. 1** Prague Security Studies Institute (PSSI) global map of space transactions of China and Russia as of February 2020 (does not include the Arctic and Antarctica)



**Fig. 2** PSSJ map of space transactions of China and Russia in the Arctic as of February 2020 (does not include the Arctic and Antarctica)



**Fig. 3** PSSl map of space transactions of China and Russia in Antarctica as of February 2020 (China in red, Russia in blue)

## Africa

Both Russia and China have assisted a number of African countries in establishing, or expanding, their space activities. Russia has worked with Angola, Algeria, Egypt, and South Africa and China has reached out to Algeria, Democratic Republic of Congo, Egypt, Ethiopia, Mozambique, Namibia, Nigeria, Sudan, Tunisia, and Uganda. In all of these cases, space ground infrastructure was provided, often through subsidized lending arrangements or even taking stakes in local companies.

Russia, for example, launched a satellite for Egypt in 2014 and also assisted in the development of their third Earth observation (EO) satellite that was launched in 2019 from Baikonur. It has offered engineering and other assistance to Ethiopia and helped South Africa in developing a satellite surveillance program.

Notable examples of China's activities in Africa are those in Nigeria. China entered Nigeria's space sector in 2004, manufacturing Nigeria's first communications satellite, NigComSat-1 (based on the Sinosat-2), which was launched in 2007. It failed after 18 months in orbit. Its replacement, NigComSat-1R, was launched in 2011 (Krebs 2017). Both satellites were built and launched under a contract with the state-controlled China Great Wall Industry Corporation (CGWIC), and the second satellite was subsidized 100% by China. It was the first time that China had reached out to a foreign country in this fashion and the first time that CGWIC provided all aspects of in-orbit delivery of a satellite for an international customer. This means China also provided two ground stations (one tracking station in Kashi, China, and one fully operational station in Abuja, Nigeria), training of personnel, financing, and insurance. In 2018, China agreed to finance (through the Export-Import Bank of China) the building of two new communication satellites, but in exchange for CGWIC's stake in state-owned NigComSat Ltd. (Nigeria's satellite communications operator and service provider). China also offered to possibly send a Nigerian astronaut to space in the 2030s.

The Nigeria example demonstrates that a recipient country can become largely dependent on its benefactor (China in this case) for its space program through this strategy of offering a complete "package deal." In a similar fashion, China has offered a satellite "package deal" to Ethiopia, Algeria, Sudan, and Congo. As for Russia, it offered a package deal to Angola and Egypt.

## Latin America

Both China and Russia successfully built and operate space infrastructure in this region. There is a robust increase in China's influence in Latin America, including through promises and agreements to provide space-related technology, expertise, and services. China has worked with Argentina, Bolivia, Brazil, Chile, Cuba, and Venezuela.

A controversial project was built by the China Harbour Engineering Company (CHEC), a subsidiary of People's Liberation Army (PLA)-affiliated China Communications Construction Company (CCCC), in Argentina – a satellite tracking,



telemetry, and command station in the Patagonia region, operational since 2017. CHEC is also involved in illegal island-building, and the militarization of same, in the South China Sea. China was able to secure a 50-year lease agreement of the land and facility and does not permit the entry of local officials. It also does not employ local personnel (Londoño 2018). The Neuquen TT&C station in Argentina is in the proximity of a number of infrastructure assets constructed by China in South America, the Fibre Optic Austral in Chile and the China-funded multi-billion-dollar turnkey railway and infrastructure projects in Argentina (Giri 2018). China also built a 60 cm-diameter telescope which resides in the Observatorio Astronomico “Felix Aguilar” (OFA) of the National University of San Juan (UNSJ). It provides data to the International Laser Ranging Service (ILRS). Another China-Argentina Radio Telescope (CART) is planned to be completed by June 2020.

More recently, an Argentinean company, Satellogic (developing a constellation of EO satellites with panchromatic, hyperspectral, multispectral and infrared capabilities), announced that it would launch its fleet of spacecraft on Chinese rockets under a contract with CGWIC. It is the largest single contract for Chinese launch industry in the international commercial market in more than 20 years (Clark 2019). The first two satellites were launched in January 2020.

Brazil is subject to US export control-related restrictions and indirectly affected by the US ban on space commerce with China. It has viewed collaboration with China and Russia in space as fundamental to its efforts to overcome bottlenecks related to the development of its space program (without any apparent concern over the country’s dependency on China and Russia in this strategic sector).

The flagship project of Beijing’s space collaboration with Brazil is the China-Brazil Earth Resources Satellites CBERS program. It is a collaboration between CAST (China Academy of Space Technology) and INPE (Instituto de Pesquisas Espaciais). China provided the technology, launch service, and subsidized financing. Data from the project have been shared since 2004, with third parties (ESA 2019).

Russia was the first to offer collaboration to Brazil in the area of global navigation. As of February 2020, Brazil hosted four GLONASS ground stations on its territory (the largest number outside Russia). Besides Brazil, Russia established GLONASS stations in Argentina, Ecuador, Nicaragua, and Venezuela. China is also seeking to launch collaboration with Brazil on its global satellite navigation system, BeiDou (which it asserts will be global by 2020) (Selding 2015). Russia also partnered with Brazil on its Russian telescope at Pico dos Dias Observatory in Brazopolis, Minas Gerais, operational since 2018. This electro-optical facility is designed to help fill the observation gaps in the geostationary orbit. Russia is reportedly planning to deploy an optical-electronic monitoring station in Chile, Mexico, and South Africa (Ibeh 2019).

Cuba, not surprisingly, hosted a large Russian signals intelligence facility between 1962 and 2002. It is said to have reopened in 2014 (Kelley 2014). Interestingly, that same year Russia wrote off some 90% of Cuba’s \$32 billion Soviet-era debt. Currently, Cuba’s largest international creditor and trading partner is, perhaps not surprisingly, China. In May 2018, satellite images revealed a newly

constructed radome within the signals intelligence base in Bejucal, Cuba. It is believed that Beijing financed this new facility (Lee 2018).

China also seeks to expand its space observation capabilities through its collaboration with Chile, establishing an astronomical research center at the Catholic University of Chile in 2013 and a plan to build its own observatory some 30 km from Chile's Paranal Observatory. As Chile has relatively good governance and strong institutions, however, China may not have gotten a preferential deal, typically involving public procurement regulations beneficial to Chinese companies, or Chinese loans and investments (Ellis 2017).

When it comes to the telecommunications sector in Latin America, China delivered complete packages (involving construction, financing, delivery, ground stations, and operations) to Bolivia, Venezuela, Cuba, and Uruguay. Argentina, Bolivia, Brazil, and Venezuela are all laboring under a troubling degree of space sector dependency with a common thread of China financing their projects through direct investments.

## Europe

Unlike in Africa and Latin America, where China, and to a lesser degree Russia, have been frequently offering vertically integrated space sector packages (partial or complete), including large-scale subsidized financing, their approach in the developed, democratic countries is more subtle and incremental, often involving seemingly benign scientific research/development initiatives, academic exchanges, individual commercial contracts, or broader funding commitments beyond the space sector.

Russia has benefited from its established ties in Europe, especially in the launch subsector. Germany, France, Spain, and the Netherlands have all been recipients of Russia's launch services. For instance, in February 2014, TsSKB-Progress signed a \$400 million supply agreement with Arianespace to provide a batch of seven Soyuz-ST rockets for launch from Kourou in French Guiana. This agreement was built on a previous arrangement between Roscosmos and the French company to launch "mid-class Soyuz-ST rockets over 15 years" (Nowakowski 2016). Russian VNIIEM Corporation also managed to secure an agreement in the EO subsector when it signed a cooperation protocol with a British company Surrey Satellite Technology in 2015 "for the creation of a small Earth remote-sensing (ERS) satellite" (Glavkosmos 2019).

There are interesting cases of corporate acquisitions by China in Germany. For example, on June 19, 2018, it was announced that Fosun International had agreed to acquire FFT Produktionssysteme GmbH & Co. from ATON GmbH for an undisclosed sum. Subsequently in August 2018, Fosun won regulatory approval from the European Commission for the acquisition, as it was deemed that no competitive concerns would arise (European Commission 2018). Similarly, in 2018, Changzhou QFAT Composite Material, a subsidiary of China Iron and Steel Research Institute, acquired aerospace firm Cotesa after the approval of German

regulators in April 2018 (Xinhua 2018). Another acquisition of the controlling 94.55% stake of the robotics firm Kuka by Midea in 2016 demonstrates that such acquisition can quickly turn into an opening for other Chinese entities to enter the local market (Taylor 2016). Within a year from the acquisition, Kuka signed a memorandum of understanding with a Chinese company Huawei to “deepen their global partnership” (Williamson 2017). Many experts believe that Huawei represents a serious national security risk.

A similar effort was discovered in Ukraine. The Beijing-based Skyrizon acquired the majority stake in Ukraine’s aerospace company Motor Sich in 2017, following a PLA contract with Motor Sich for 250 jet engines for JL-10/L-15 jets, a deal worth \$380 million concluded in 2016 (Wang 2018). As the Pentagon, NATO officials, and G7 diplomats raised concern over Skyrizon interest in Motor Sich, Ukraine’s antitrust authority eventually launched an investigation into the case to potentially block the deal. As of late February 2020, the antitrust authority says it might have a strong case against the deal and it appears that it could be canceled (Gorchinskaya 2020).

As a backdrop to these developments, in November 2017 Ukrainian representatives signed a long-term cooperation program with their Chinese counterparts that included some 70 projects that involve, among other areas, “implementation of China’s Lunar Exploration Program, a mission to study the planets of the solar system, new materials development, and remote sensing” (Interfax-Ukraine 2017). Russia’s complex involvement in Ukraine, following the 2014 invasion of its southeastern territory, involved the reintegration of some of its Soviet-built infrastructure into its ground station network (Foust and Bodner 2016) in an extraordinary breach of international law.

Belarus is a prime example of a country’s space sector being shaped by both China and Russia. As a former Soviet republic, its space sector has been closely tied to that of Russia. China made its foray into Belarus through its state-owned enterprises, monitored by a special Committee established by Belarus called the Belarusian-Chinese Intergovernmental Committee on Cooperation. The 91.5 km<sup>2</sup> “Great Stone Industrial Park” located outside Minsk was stood up in 2010 under an agreement between Belarus Economy Ministry and China CAMC Engineering Co. Ltd. (CAMCE) and is overseen by the China-Belarus Industrial Park Development Company (JSC), owned 60/40 by the Chinese and Belarusian governments, respectively. Chinese telecom giants ZTE and Huawei have been heavily involved in the development of this industrial park. Both companies have a history of assisting China’s intelligence operations and the alleged theft of intellectual property (Pai 2019).

PLA-affiliated China Aerospace Science and Technology Corporation (CASC) signed a letter of intent in March 2018 to become an anchor company in the industrial complex (Belta 2018a). In addition, the China-Belarus Cooperation Center for Science and Technology Achievement is to be built by another Great Stone resident, China No. 15 Metallurgical Construction Group (15MCC), and “funded using an economic and technical assistance grant from the Chinese government” (Belta 2018b).

The same Chinese entity (CAMCE) overseeing Chinese investment into Great Stone in Belarus signed a memorandum of understanding with Lithuanian Kaunas Free Enterprise Zone regarding the development of a pilot free trade zone, which should involve funding for research and development in biotechnology, information technology, space research, and photonics. While the current status of the joint project is not available in the open source, the Chinese side has made a connection between the zones in Lithuania and Belarus saying: “Minsk and Kaunas will be developed as inland terminals for the North and Baltic Seaports (especially Klaipeda Seaport)” (Rail Working Group 2016).

Belarus is also a recipient of a comprehensive package deal involving the construction, launch, training, ground station, and temporary management of a communications and broadcasting satellite, Belintersat-1 offered through the China Great Wall Industry Corporation (CGWIC). The satellite’s launch (from Xichang) in January 2016 coincided with a sharp increase in exports (75.5% in the first 9 months) from the Belarusian military-industrial complex to China. This was the first CGWIC contract with a European client. (CGWIC previously launched six other satellites for international clients). It was also the first time that CGWIC got involved in the satellite’s operations (Hill 2011).

Belarus stands as a post-Soviet state that is largely compelled to remain Moscow’s strategic ally through economic, political, and diplomatic leverage, as well as hybrid operations. Interestingly, Belarus has sought to attract China’s investment possibly to help offset Russia’s inordinate influence. In 2018, Minsk was the destination of Chinese Defense Minister Wei Fenghe’s first foreign visit (together with Moscow), demonstrating Beijing’s strategic interest in this region. Although it may seem as a smart move to reduce traditional Russian domination, Minsk seems to be on the path of full space sector dependency on Beijing and Moscow.

## The Arctic

As an Arctic state, Russia’s space-related activity in the Arctic largely remains confined to its vast amount of its claimed Arctic territory, and, as such, is not analyzed in this article. That said, Russian companies have been identified as having other business ties in certain Arctic states, including Svalbard.

China’s space activities in the region have been expanding. In December 2018, the relatively new Ministry of Natural Resources (MNR), which now oversees the Chinese Arctic and Antarctic Administration (CAA), launched the “Arctic Environment Satellite and Numerical Weather Forecasting Project.” According to MNR, it is to assist China’s role in the governance of the Arctic and in the building of the Polar Silk Road (Eiterjord 2019). China currently has its stations in Kiruna (Sweden), Karholl (Iceland), Ny-Ålesund (Svalbard), and Longyearbyen (Svalbard), and plans to establish ones in Finland (Sodankyla) and Greenland (Nuuk).

The China Remote Sensing Satellite North Polar Ground Station (CNPGS) in Kiruna, Sweden, is the first Chinese overseas EO satellite data receive station. CAS declared CNPGS in

Kiruna to be an important part of China's Gaofen project (launched in 2010) – a global EO satellite network to be completed in 2020. Concerns have been raised about its potential dual-use purpose. In January 2019, the Swedish Defense Ministry's Defence Research Agency (FOI) publicly expressed a concern that the ostensibly civilian cooperation with China could, in fact, be controlled by the PLA and used to supplement military surveillance of the Arctic region with implications for Sweden's national security (Hinshaw and Page 2019).

The China-Iceland Arctic Science Observatory (CIAO) in Karholl, Iceland, is jointly operated by PRIC and the Icelandic Centre for Research (Rannis). The facility, not far from the Icelandic port town Akureyri, has been operational since October 2018. China's Ny-Ålesund Yellow River Station on Svalbard Island, operational since 2004, has the world's largest space physics observatory and is able to accommodate 37 personnel in summer and 4 in winter (the highest occupancy of any other country with facilities there).

China's interest in Finland spiked in the period of its Chairmanship of the Arctic Council from 2017–2019, resulting in, among other developments, a China-Finland Joint Action Plan (2019–2023), which laid the groundwork for additional Chinese investment in the country going forward (MFA Finland 2019). Implementation of this action plan has included an agreement between Chinese RADI and Finnish Meteorological Institute to establish a joint Research Center for Arctic Space Observations and Data Sharing to be built in Sodankyla, Lapland.

With regard to Greenland, although it has resisted, to date, Chinese demarches, it remains a target for Chinese investment. In 2017, rather discreetly, a Chinese-funded satellite ground station and a research facility were launched in Greenland, a collaboration between a local Greenland Institute of Natural Resources and Global Change and Earth System Science Research Institute of the Beijing Normal University (BNU) (CAS 2018).

## Antarctica

With regard to space-related activities in Antarctica, Russia's GLONASS stations and Chinese BeiDou stations have been installed in this region and both countries have research stations there some of which have space capabilities. China's research stations include the Changcheng (Great Wall), Zhongshan (established in 2010), Kunlun (since 2013), and Taishan (since 2014). The Polar Research Institute plans to build China's fifth station on the Inexpressible Island with construction to be completed by 2022. This research station would be close to the world's largest Antarctic station – McMurdo Station of the United States as well as New Zealand's Scott Base (Liu 2018).

Russia reopened in 2006 its Molodyozhnaya Research Station, the Soviet Union's largest station in Antarctica. Russia's most important location in Antarctica is its newer Progress station. Its other stations include the Vostok Research Station, Novolazarevskaya Research Station, Bellingshausen Research Station, and the oldest Mirny Research Station. The activities of both countries in Antarctica demonstrate their determination to bolster their presence in this strategic outpost.

## The Middle East

Russia and China's space presence in this region has sharply increased in the past few years with the signing several state-to-state Memorandum of Understanding (MoUs) on future collaboration. Russia, for example, has used human space flight as a diplomatic tool. The United Arab Emirates (UAE) has already had their astronaut sent to the ISS in September 2019 with Russian assistance. Saudi Arabia and Bahrain are in talks with Roscosmos, and Egypt and Iran are also believed to be interested in having their astronauts sent into orbit by Russia.

Russian activity in this region was recorded in the UAE, Israel, Iran, and Turkey. Roscosmos and other Russian companies (i.e., VNIEM and Barl) are assisting Iran as it seeks to create its own remote sensing capabilities. The assistance comes in many forms, including the supply of parts and technology, ground network equipment, and potential launches of spacecraft which could be provided by Roscosmos.

Iran's first satellite, Sina-1, was built and launched in 2005 by Russia (NPO Polyot). At that time, information concerning the satellite's payload was not disclosed. Roscosmos is to potentially provide future launches as Iran struggles to build its own reliable launch infrastructure, despite being ostracized from the international community for its nuclear program. Russia also signed a deal with Iran (2005) promising to build and launch two telecommunications satellites, Zohreh 1 and Zohreh 2. The deal was terminated for unknown reasons but could possibly be resurrected.

Russia's collaboration with the UAE takes advantage of the UAE's strategy of funding high-tech projects to promote the country's capabilities. Moscow can offer its space hardware and expertise, including in the Space Situational Awareness (SSA) SSA and GNSS subsectors. Research and development projects include, for example, the "Martian Town" project which is to be built in Dubai by 2023.

Chinese involvement in the Middle East has included collaboration with Israel, Saudi Arabia, and Turkey, largely through CGWIC. The company facilitated China's collaboration with the King Abdulaziz City for Science and Technology (KACST) of Saudi Arabia. KACST developed an optical micro-camera that was launched in May 2018 on one of China's Longjiang (Dragon River) microsattellites for lunar orbit operations. It was part of China's Queqiao Chang'e-4 relay satellite mission in May 2018. China also launched the Saudi-made SaudiSat 5A and SaudiSat 5B EO satellites in December 2018, demonstrating its reliable low-Earth orbit (LEO) launch services.

Interestingly, the development of the two SaudiSat-5 satellites was based on the Saudi Arabia-Belarus agreement from May 2016, in an effort to bolster Riyadh's own manufacturing capabilities (Barbosa 2018). In December 2012, CGWIC also assisted Turkey in the launch of its EO satellite (GÖKTÜRK-2). China has also sought to expand its GNSS presence in the Middle East and North Africa (MENA) region through its "BeiDou Center of Excellence" in Tunis, Tunisia.

## South and Southeast Asia

Both Beijing and Moscow have a formidable network of partnerships in this region. China has provided assistance to Afghanistan, Bangladesh, Cambodia, Indonesia,

Laos, Pakistan, Sri Lanka, and Thailand. Overall, most of China's activities involved construction and launch of telecommunications satellites (Afghanistan, Pakistan, Sri Lanka, Cambodia, and Indonesia), often through some form of package deal. Other transactions focused on sole launches (e.g., Palapa-D, SupremeSAT-I, PakTES-1A) and the use of BeiDou system (e.g., construction of BeiDou stations in Pakistan or lease of BeiDou for Thailand).

Space sectors dependent on China include those of Sri Lanka (SupremeSAT, Pallekele Space Academy, etc.), Indonesia (Palapala-N1), Cambodia (Techo-1), and Pakistan (PakSat-1R). Pakistan, Thailand, and Sri Lanka also facilitate BeiDou's coverage, hosting stations on their territories. Bangladesh is the only country in which CGWIC lost a bid for the manufacturing and launch of Bangladesh's first telecommunications satellite, Bangabandhu Satellite-1, to Thales Alenia Space (Shamrat 2018).

Russia has worked with Bangladesh, Indonesia, India, the Philippines, and Vietnam. Relations with India are most extensive. In 2010, Russia and India signed an intergovernmental agreement on granting India access to the encrypted high-accuracy military GLONASS signal (Sputnik 2018). In May 2015, Roscosmos signed an MoU with the Indian Space Research Organization (ISRO) to increase their cooperation in a series of subsectors (e.g., satellite navigation, launch vehicle development, remote sensing, the use of ground infrastructure) and provide India's Space Program with GLONASS technology (TASS 2018). Out of these agreements emerged several potential projects that are in their initial stages. These include a joint communications satellite, creating a remote sensing constellation, training of Indian personnel to send them to the International Space Station on board a Russian spacecraft, monitoring of Indian Railways, and construction of ground stations in India (including Russian global navigation satellite system (GLONASS) stations) (Cozzens 2019).

## Western, Central, and Eastern Asia

Although China has sought to establish ties in this region, and reached out to Armenia, Azerbaijan, Turkmenistan, and Armenia, Russia remains the more prominent space player in this region, working with Armenia, Azerbaijan, South Korea, Kazakhstan, and Uzbekistan.

Russia has been historically active in Kazakhstan mainly because of the existing launch infrastructure located in Baikonur, the lease of which expires in 2050. Kazakhstan was granted access to GLONASS military signal in 2018. (India (in 2010) and Algeria (in 2019) also received access to the GLONASS military signal.) A GLONASS station was also opened at the Byurakan Observatory in Armenia, which included some modernization of the existing station. Following this transaction, Russia, aiming to further strengthen its ties with Armenia, promised to train an Armenian astronaut for a mission to the International Space Station.

Russia also recently reached out to Uzbekistan. It was reported on May 1, 2018, that Roscosmos offered the Uzbek State Space Research Agency (Uzbekcosmos) to

finance a program that would enable the country to launch its first satellites. Shortly thereafter, a proposal on a trilateral (Russia, Uzbekistan, and Kazakhstan) satellite launch was tabled (SpaceWatchGlobal 2018).

---

## Top Space Sector Capture Trends

When analyzing partnering arrangements described in section two of this article, there seem to be four prominent space sector capture trends. They include vertically integrated package deals (e.g., in Angola, Belarus, Brazil, Congo, Ethiopia, Bolivia, Pakistan, Nigeria, Algeria, Venezuela); the active involvement of China and Russia in the Arctic and Antarctica; China's global space power projection through EO and space observation partnerships; and expanding the number of GNSS (GLONASS and BeiDou) ground stations abroad enhancing the capabilities of the respective systems.

The package deals are a hallmark of Chinese and Russian influence attempts and have been most evident in the telecommunications subsector (but also found, for example, in the EO subsector). While the general pattern of the package deals is similar across the board, the number and type of components in each offer varies.

China has been a driver of multilateral Space and Earth observation partnerships. China leads the international Asia-Pacific Ground-based Optical Space Objects Observation System (APOSOS) initiative, launched through the Asia-Pacific Space Cooperation Organization (APSCO). The stated goal is to build a global optical observation network with at least one facility in each of the APSCO Member States and elsewhere. China has sensors in all eight APSCO member countries, as well as in Brazil and Ukraine. Mexico joined the APOSOS network in 2017 (IDA 2018).

The primary objective of this organization is to build a data sharing platform and use existing infrastructures from Member States. A second objective is to bring new capabilities to the table and extend the ability to observe MEO and GEO. It is to be operated under APSCO observation mission management department. For example, new telescopes (manufactured by the Changchun Institute of Optics, Fine Mechanics and Physics of CAS) have been completed and declared functional in Iran, Pakistan, and Peru.

China has also tied its economic and strategic interests to the grouping of Brazil, Russia India, China, and South Africa (BRICS) nations, providing financial backing to a sizeable portion of their activities. This includes the first BRICS space project – sharing of EO data with an intention to eventually build a remote sensing satellite constellation. While a specific timeline has not been made available, the current plans are for the project to have two phases: (1) the creation of a remote sensing data-sharing system, making the data from each of the member countries' existing EO satellites available to all the other members; and (2) the creation of a new EO satellite constellation (Campbell 2017). There is also an EO collaboration between Europe and China through the Dragon program (currently in its 4th iteration) between MOST's National Remote Sensing Centre of China and the European Space Agency (ESA).



Spearheaded by China and Russia, BRICS was configured as a platform for engagement of emerging market economies and developing countries. Initially, the initiative struggled to fund itself, but the creation of the BRICS Development Bank, now called the New Development Bank (NDB), based in Shanghai, represented an important pivot operationally. In April 2017, Brazil was the recipient of the bank's first development loan. Together with the Asian Infrastructure Investment Bank and the Silk Road Fund, NDB is a key investment tool for China's power projection strategy abroad (Reuters 2018).

With regard to the GNSS sector, both Russia and China continuously work on global expansion of their respective systems. Russian President Vladimir Putin prioritized the GLONASS system's restoration in the early 2000s. The full constellation of satellites was reestablished by 2011. GLONASS satellites have undergone several upgrades over the years, the latest being the GLONASS-K. The GLONASS stations have been (or are planned to be) placed in Antarctica, Argentina (planned), Armenia, Cuba (planned), Ecuador (planned), India (two stations, both planned), Kazakhstan (one existing and one planned), Nicaragua, South Africa, South Korea (envisioned), UAE (planned), and Venezuela (planned).

With regard to China, on December 27, 2018, China's BeiDou Navigation Satellite System (BDS) was declared to be providing global service as the construction of the BDS-3 primary system had been completed. China wants BeiDou to become an alternative to America's Global Positioning System (GPS). The BeiDou applications are also promoted through the Belt and Road Initiative (BRI). The more widespread use of Russia's and China's GNSS will help them integrate these countries into their respective economic and military orbits.

---

## Key Findings

Although it is not possible to accurately assess the precise number and status of all existing space partnerships that China and Russia have concluded globally with the use of open source materials, it has been possible to determine that the number of these partnerships has expanded substantially, especially on the part of China. A Chinese media source asserts that, as of April 2018, China had signed 121 space cooperation agreements with 37 countries and four international organizations (MFA PRC 2018). Back in 2016, according to the State Council Information Office on China's space activities, China had signed 43 space cooperation agreements with 29 countries, space agencies, and international organizations (SCIO PRC 2016). If accurate, this would mean an increase of 78 international cooperation agreements over about 15 months. PSSI has identified Chinese space relationships with 60 countries as of February 2019.

Russia has been less transparent when it comes to declaring publicly the number of international space partnerships it has concluded. It has mentioned international cooperation in relation to its technological development goals in its "Russian Federal Space Program 2016–2025" (Roscosmos 2016). Russia has mostly focused on reviving, or maintaining, its post-Soviet ties. CIS states are important targets

(especially Belarus, Kazakhstan, and Armenia, but also Azerbaijan, Moldova, Tajikistan, Turkmenistan, and Uzbekistan) (Roscosmos 2020). PSSI unearthed Russian space partnerships with 44 countries.

Overall, Chinese and Russian economic and financial activities in various regions indicate that space sector partnerships that create various levels of dependencies (and even full-scale space sector capture) have been vigorously pursued with respect to both developing and developed countries. As democratic countries have more rigorous requirements for transparency, accountability, and the rule of law, a more subtle, incremental approach is evident (e.g., projects related to scientific research/development, academic exchanges, or individual commercial contracts).

The research suggests that China and Russia enter into space partnerships globally for two main reasons: (1) because the recipient state is in an important, or even strategic, geographic location for enhancing Chinese/Russian space capabilities (e.g., for GLONASS/BeiDou, SSA, EO); and (2) a country has strategic importance that a space partnership helps leverage (e.g., a country's energy resources, mineral wealth, supportive geopolitical policy positions). In some cases, these motivations are co-mingled, such as the case of the Arctic countries (e.g., Greenland).

The second pattern of behavior described above (where space considerations are not the prime mover) most often occurred in less economically successful, but resource-rich, countries (e.g., Bolivia, Nigeria, Venezuela), or countries that are geographically and/or geopolitically strategic for China or Russia (e.g., Pakistan for China, Iran for Russia, and Cuba for both countries). In the case of China, some of these recipient countries (e.g., Belarus, Cambodia, Laos, and Pakistan) are valued clients of its BRI, without a direct linkage to space.

Incremental space sector dependencies in the developed countries are more difficult to detect and guard against (e.g., academic exchanges, scientific and research projects, broader funding commitments beyond the space sector). More visible space sector capture largely takes place via the offering of vertically integrated "package deals." On a number of occasions, China and Russia have been able to construct successfully dual-use space infrastructure and services due to hospitable political relations, corruption, and internal economic and social strife in the targeted countries (e.g., Argentina, Brazil, Cuba, Colombia, Nicaragua, Nigeria, Pakistan, Sri Lanka, Venezuela).

China and Russia generally use their state-controlled enterprises (e.g., China Great Wall Industry, Roscosmos) to penetrate a specific country's space sector. These state companies position themselves as preferred "go-to" entities. This is, in no small part, because of generous financing that often does not reflect the targeted country's creditworthiness.

The pattern of Chinese and Russian space-related transactions reveals a global approach, signaling that both countries are determined to expand their space stature and competitiveness, and close the gap with Europe and the United States. Some targeted countries receive financial backing well beyond the space sectors. Influencing/capturing the space sector is just part of a broader strategic outreach (e.g., in Bolivia).

## Conclusion

Tracking and visually mapping the international transactions of Chinese and Russian state-controlled enterprises in the space sectors of various countries revealed that Beijing and Moscow offer assistance to the nascent space programs that, in many cases, create dependencies, including a full-scale space sector capture.

Today, the implications of the active pursuit of international space partnerships globally by China and Russia to increase their influence over the space domain through such means as the offer of vertically integrated “package deals” of capabilities and services are not well-understood. The economic and financial largesse provided by these state actors, including subsidized financing, are accepted, and often even welcomed, by the recipient countries which lack their own space funding, technical expertise, and human resources, even if it exposes them to partial or complete dependency on these outside “benefactors.”

One of the risks stemming from these global networks of space dependencies is the opening for China and Russia to increasingly shape applicable rules, norms, and standards for access to, and operations in, space. This asymmetric threat to global space governance stemming from these hybrid economic and financial maneuvers needs to be better appreciated, including the underlying rationales for these activities.

The United States, Europe, and other allies, including Japan, need to also review their space partnership approaches and configure more effective and attractive offers to their nontraditional space partners to counter Chinese and Russian predatory economic and financial practices. It is clear that countries of all economic performance levels are intent on benefiting from the value provided by space. If upgraded space-related engagement and an enhanced level of support do not occur from Western countries, the void is likely to be filled – as we are already witnessing – from these nondemocratic actors, with negative consequences.

As in other domains, a sustainable model of international partnerships cannot be established without transparency, good governance, accountability, respect for national sovereignty, and the rule of law. Western nations will have to be able to demonstrate that there is a clear benefit in collaboration with countries that respect free and fair market principles and behavior versus state-controlled economies that often show little regard for such principles.

---

## References

- Barbosa R (2018) Long March 2D launches SaudiSAT-5A/B NASA space flight. NASA Spaceflight. <https://www.nasaspaceflight.com/2018/12/long-march-2d-saudisat-5a-b/>. Accessed 10 Mar 2020
- Belta (2018a) China aerospace science and technology corporation to open research center in Belarus. Belarus Telegraph Agency. <https://eng.belta.by/society/view/china-aerospace-science-and-technology-corporation-to-open-research-center-in-belarus-113476-2018/>. Accessed 10 Mar 2020

- Belta (2018b) Plans to build R&D commercialization center in China-Belarus industrial park within one year. Belarus Telegraph Agency. <https://eng.belta.by/economics/view/plans-to-build-rd-commercial-ization-center-in-china-belarus-industrial-park-within-one-year-117427-2018/>. Accessed 10 Mar 2020
- Campbell K (2017) BRICS bloc agree remote sensing space constellation project. Engineering News. [http://www.engineeringnews.co.za/article/brics-bloc-agree-remote-sensing-space-constellation-project-2017-07-04/rep\\_id:4136](http://www.engineeringnews.co.za/article/brics-bloc-agree-remote-sensing-space-constellation-project-2017-07-04/rep_id:4136). Accessed 10 Mar 2020
- CAS (2018) China, Finland to enhance Arctic research cooperation. Chinese Academy of Sciences. [http://english.cas.cn/Special\\_Reports/Belt\\_of\\_Science\\_Road\\_for\\_Cooperation/Technology\\_Cooperation/201810/t20181029\\_200564.shtml](http://english.cas.cn/Special_Reports/Belt_of_Science_Road_for_Cooperation/Technology_Cooperation/201810/t20181029_200564.shtml). Accessed 9 Mar 2020
- Clark S (2019) Chinese company inks deal to launch 90 commercial smallsats. Spaceflightnow. <https://spaceflightnow.com/2019/01/30/chinese-company-inks-deal-to-launch-90-commercial-smallsats/>. Accessed 3 Mar 2020
- Cozzens T (2019) India to host GLONASS ground station for Russia. GPS World. <https://www.gpsworld.com/india-to-host-glonass-ground-station-for-russia/>. Accessed 10 Mar 2020
- Eiterjord T (2019) China's busy year in the Arctic. The Diplomat. <https://thediplomat.com/2019/01/chinas-busy-year-in-the-arctic/>. Accessed 8 Mar 2020
- Ellis E (2017) China's relationship with Chile: the struggle for the future regime of the Pacific. Jamestown Foundation. <https://jamestown.org/program/chinas-relationship-chile-struggle-future-regime-pacific/>. Accessed 8 Mar 2020
- ESA (2019) CBERS – 1st generation. eoPortal Directory. <https://directory.eoportal.org/web/eoportal/satellite-missions/c-missions/cbers-1-2>. Accessed 5 Mar 2020
- European Commission (2018) Daily news press release 27/08/2018. European Commission. [http://europa.eu/rapid/press-release\\_MEX-18-5181\\_en.htm](http://europa.eu/rapid/press-release_MEX-18-5181_en.htm). Accessed 7 Mar 2020
- Foust J, Bodner M (2016) How Crimea fractured Ukraine's space program. SpaceNews. <https://spacenews.com/from-the-magazine-ukraines-untethered-orbital-manuevers-how-crimea-hurt-ukraines-space-program/>. Accessed 7 Mar 2020
- Giri C (2018) Version 2: mapping China's global telecom empire. Gateway House. <https://www.gatewayhouse.in/china-global-telecom-tentacles/> Accessed 9 Mar 2020
- Glavkosmos (2019) Services/earth observation data and solutions. Glavkosmos JFC. <http://glavkosmos.com/en/earth-observation/>. Accessed 7 Mar 2020
- Gorchinskaya K (2020) Ukraine prepares to snub China in aerospace Deal with U.S. help. Forbes. <https://www.forbes.com/sites/katyagorchinskaya/2020/02/17/ukraine-prepares-to-snub-china-in-aerospace-deal-with-us-help/#2aa25509328c>. Accessed 9 Mar 2020
- Hill J (2011) China wins first European satellite construction, Launch Contract. Via Satellite. <https://www.satellitetoday.com/telecom/2011/09/21/china-wins-first-european-satellite-construction-launch-contract/>. Accessed 10 Mar 2020
- Hinshaw D, Page J (2019) How the pentagon countered China's designs on Greenland. Wall Street J. <https://www.wsj.com/articles/how-the-pentagon-counterred-chinas-designs-on-greenland-11549812296>. Accessed 10 Mar 2020
- Ibeh J (2019) Russia to deploy space monitoring stations in South Africa, Mexico and Chile. Space in Africa. <https://africanews.space/russia-to-deploy-space-monitoring-stations-in-south-africa-mexico-and-chile/>. Accessed 5 Mar 2020
- IDA (2018) Global trends in space situational awareness (SSA) and space traffic management (STM). Institute for Defense Analyses, p 50. <https://www.ida.org/idamedia/Corporate/Files/Publications/STPIPubs/2018/D-9074.pdf>. Accessed 10 Mar 2020
- Interfax-Ukraine (2017) Ukraine, China approve updated bilateral program of space cooperation until 2020. KyivPost, Interfax-Ukraine News.Agency. <https://www.kyivpost.com/ukraine-politics/ukraine-china-approve-updated-bilateral-program-space-cooperation-2020.html>. Accessed 7 Mar 2020
- Kelley M (2014) Russia is reportedly reopening its Spy Base in Cuba. Business Insider. <https://www.businessinsider.com/russia-is-reportedly-reopening-its-spy-base-in-cuba-2014-7>. Accessed 9 Mar 2020

- Krebs G (2017) NIGCOMSAT 1 and 1R. Gunter's space page. [https://space.skyrocket.de/doc\\_sdat/nigcomsat-1.htm](https://space.skyrocket.de/doc_sdat/nigcomsat-1.htm). Accessed 9 Mar 2020
- Lee RV (2018) Satellite images: a (Worrying) Cuban mystery. *The Diplomat*. <https://thediplomat.com/2018/06/satellite-images-a-worrying-cuban-mystery/>. Accessed 2 Mar 2020
- Liu N (2018) What does China's fifth Research Station mean for Antarctic governance?. *The Diplomat*. <https://thediplomat.com/2018/06/what-does-chinas-fifth-research-station-mean-for-antarctic-governance/>. Accessed 10 Mar 2020
- Londoño E (2018) From a Space Station in Argentina, China Expands its Reach in Latin America. *New York Times*. <https://www.nytimes.com/2018/07/28/world/americas/china-latin-america.html>. Accessed 5 Mar 2020
- MFA Finland (2019) Joint action plan between China and Finland. The Ministry of Foreign Affairs of Finland. <https://um.fi/documents/35732/0/Joint+Action+Plan+2019-2023+%283%29.pdf/bd639013-a815-12d2-ae44-4bc50ded7a97>. Accessed 9 Mar 2020
- MFA PRC (2018) China strengthens international space cooperation. Ministry of Foreign Affairs of the People's Republic of China. <https://www.fmprc.gov.cn/zflt/eng/jlydh/mtsyt/1555457.htm>. Accessed 9 Mar 2020
- Nowakowski T (2016) Arianespace to launch Soyuz rocket with European satellites. *SpaceFlight Insider*. <https://www.spaceflightinsider.com/organizations/arianespace/arianespace-launch-soyuz-rocket-european-satellites/>. Accessed 7 Mar 2020
- Pai Ajit (2019) Protecting National Security and public safety. Federal Communications Commission. <https://www.fcc.gov/news-events/blog/2019/10/28/protecting-national-security-and-public-safety>. Accessed 16 Mar 2020
- Rail Working Group (2016) Kaunas free economic zone joins the rail working group rail working group. Rail Working Group. <https://www.railworkinggroup.org/kaunas-free-economic-zone-joins-the-rail-working-group/>. Accessed 9 Apr 2019
- Reuters (2018) BRICS development bank to expand lending to private sector. *Reuters, Business News*. <https://www.reuters.com/article/us-china-brics-bank/brics-development-bank-to-expand-lending-to-private-sector-idUSKCN1IU0P2>. Accessed 10 Mar 2020
- Robinson J (2018a) Competition for international space partnerships. *Prague Security Studies Institute, Prague*, p 6. [http://www.pssi.cz/download/docs/617\\_sagar2018-presentation-robinson.pdf](http://www.pssi.cz/download/docs/617_sagar2018-presentation-robinson.pdf). Accessed 26 Nov 2018
- Robinson J (2018b) Cross-domain responses to space hybrid provocations via economic and financial statecraft. In: USSTRATCOM 2018 deterrence and assurance academic Alliance conference, March 2018. [https://www.stratcom.mil/Portals/8/Documents/AA\\_Proceedings/3.pdf?ver=2018-10-04-141147-287](https://www.stratcom.mil/Portals/8/Documents/AA_Proceedings/3.pdf?ver=2018-10-04-141147-287). Accessed 9 Mar 2020
- Robinson J (2018c) Europe's preparedness to respond to space hybrid operations. *Prague Security Studies Institute, Prague*, p 4. [http://www.pssi.cz/download/docs/590\\_europe-s-preparedness-to-respond-to-space-hybrid-operations.pdf](http://www.pssi.cz/download/docs/590_europe-s-preparedness-to-respond-to-space-hybrid-operations.pdf). Accessed 9 Mar 2020
- Robinson J, Robinson R, Davenport A, Kupkova T, Martinek P, Emmerling S, Marzorati A (2019) State actor strategies in attracting space sector partnerships: Chinese and Russian economic and financial footprints. *Prague Security Studies Institute, Prague*. [http://www.pssi.cz/download/docs/686\\_executive-summary.pdf](http://www.pssi.cz/download/docs/686_executive-summary.pdf). Accessed 4 Mar 2020
- Roscosmos (2016) The main provisions of the Federal Space Program 2016–2025. *State Space Corporation ROSCOSMOS, Moscow*. <https://www.roscosmos.ru/22347/>. Accessed 9 Mar 2020
- Roscosmos (2020) Intergovernmental agreements and commissions for economic, scientific and technical cooperation. *Roscosmos*. <https://www.roscosmos.ru/22887/>. Accessed 7 Mar 2020
- SCIO PRC (2016) White paper on China's Space Activities in 2016. *The State Council Information Office of the People's Republic of China*. [http://www.spaceref.com/news/viewsr.html?pid=49722;http://english.scio.gov.cn/whitepapers/2017-01/10/content\\_40535777.htm](http://www.spaceref.com/news/viewsr.html?pid=49722;http://english.scio.gov.cn/whitepapers/2017-01/10/content_40535777.htm). Accessed 10 Mar 2020
- Selding P (2015) Brazilian government bypassing the US as it builds out a space sector. *SpaceNews*. <https://spacenews.com/brazil-bypassing-the-us-as-it-builds-out-a-space-sector/>. Accessed 8 Mar 2020

- Shamrat AS (2018) Bangladesh joins the space age. YaleGlobal, Yale University. <https://yaleglobal.yale.edu/content/bangladesh-joins-space-age>. Accessed 10 Mar 2020
- SpaceWatchGlobal (2018) Uzbekistan widens partnerships for emerging space programme. SpaceWatch.Global. <https://spacewatch.global/2018/11/uzbekistan-widens-partnerships-for-emerging-space-programme/>. Accessed 9 Mar 2020
- Sputnik (2018) Russia Grants Kazakhstan access to military satellite signal – space agency. Sputnik News. <https://sputniknews.com/military/201808041066939986-russia-kazakhstan-military-satellite-signal/>. Accessed 9 Mar 2020
- TASS (2018) Russia’s Roscosmos invites India to cooperate in manned space missions, satellite program. TASS Russian News Agency. <http://tass.com/science/1023084>. Accessed 9 Mar 2020
- Taylor E (2016) China’s Midea receives U.S. green light for Kuka takeover. Reuters. <https://www.reuters.com/article/us-kuka-m-a-mideamidea-group-idUSKBN14J0SP>. Accessed 9 Mar 2020
- Wang B (2018) Ukraine helping South Korea, China and Canada With Rockets or Jets or Both. Nextbigfuture. <https://www.nextbigfuture.com/2018/12/ukraine-helping-south-korea-china-and-canada-with-rockets-and-jets.html>. Accessed 9 Mar 2020
- Williamson J (2017) Huawei and KUKA forge new smart manufacturing deal. The Manufacturer. <https://www.themanufacturer.com/articles/huawei-and-kuka-forge-new-smart-manufacturing-deal/>. Accessed 3 Mar 2020
- Xinhua (2018) German government gives Chinese AT&M’s takeover of Cotesa green light: report. Xinhua Net. [http://www.xinhuanet.com/english/2018-04/26/c\\_137139362.htm](http://www.xinhuanet.com/english/2018-04/26/c_137139362.htm). Accessed 9 Mar 2020



# Space Export Control Law and Regulations 11

Ulrike M. Bohlmann and Gina Petrovici

## Contents

Introduction .....	186
Terminology .....	186
International Legal Regimes .....	189
The Melee of International Legal Instruments on Export Control .....	190
The Specificities of the Outer Space Regime .....	192
National and Regional Legal Regimes .....	194
The Export Control Regime of the United States .....	194
Export Regulations of the European Union .....	200
The Export Control Regulations of the European Space Agency .....	203
Conclusions .....	205
References .....	206

## Abstract

The world continues to face an increasing demand for dedicated space applications. Global partnerships and cooperation provide the baseline for numerous space missions. International cooperation entails peaceful exploration, exploitation, and use of outer space since the early post-Cold War years. Space technology is dual-use by nature as it is serving scientific or even commercial interests on

---

The views expressed are purely personal and do not necessarily reflect the view of any entities with which the authors may be affiliated. Legal developments up to 28 February 2019 have been taken into account.

---

U. M. Bohlmann (✉)  
European Space Agency (ESA), Paris, France  
e-mail: [ulrike.bohlmann@esa.int](mailto:ulrike.bohlmann@esa.int)

G. Petrovici  
German Aerospace Center (DLR), Bonn, Germany  
e-mail: [gina.e.petrovici@googlemail.com](mailto:gina.e.petrovici@googlemail.com)

the one hand and strategic, defense-related objectives on the other. A functioning and reliable system for space export controls is a prerequisite for a well-functioning international space industry. This contribution sheds light on the relevant international, regional, and national legal mechanisms and their respective effects on the space industry.

---

## Introduction

Since the inception of space activities, with the launch of Sputnik 1, enduring scientific and technological development ensured the success of outer space activities.

Outer space developed as an enabler and outer space activities, and their applications are tremendously important tools to answer the needs of modern society. The strategic and political objectives of outer space activities have always been intrinsically linked to the economic success and social returns (ESA Space Economy 2019). The Satellite Industry Association detected a global growth of satellite industry revenues of \$ 268.6 billion (SIA 2019), and Europe's space sector is facing an extraordinary long series of growing sales, with a growth of sales to European customers of € 703 million (Aerospace and Defence Industries Association of Europe (ASD) EUROSPACE 2018). "Taking together Europe's defense and civil aeronautics, exports are at the same order of magnitude as the US" (ibid.). Export control systems are closely connected to the realm of international cooperation and foreign policy, to national security, and, as for the technical aspects, to space technology and its underlying technical knowledge. Understanding the logic behind the export control systems necessitates considering all four of these areas and their respective interconnections. While space technology determines the object of export controls and its practical scope, national security and international cooperation form the nature of the rules with their political impact. At the same time, it is precisely space technology and its characteristics that influence the national approaches toward its export controls and the willingness to cooperate on an international level. Although these interrelations are apparent and recognized, an analysis revealing their structure and inner functioning is necessarily multifaceted. The tangled connections give rise to rather complex and very heterogeneous systems of export control rules and its further development.

---

## Terminology

Export control regulations are considered to be part of foreign trade law (Wegner et al. 2006, p. 21). More precisely, export controls can be understood as segment of commercial administrative law (Tietje 2009, aup.681). Governments exercise export controls as a means to promote foreign policy and commercial interests and to protect strategic industrial sectors as well as national security and the



nonproliferation of sophisticated weapons and weapons of mass destruction (WMD) (Hertzfeld and Jones 2011).

For the sake of this chapter, we define *export controls* as the restriction on the export of goods or services imposed by the exporter's own country. Export controls apply to a variety of items: chemical, biological, nuclear, military, and dual-use in nature (Aubin and Idiart (2011), pp. 1–18). The laws and regulations governing export controls are in fact posing an exception to the free trade principles of international commercial exchanges. Thus, entities involved in trade of controlled goods and services are obliged to follow and comply with the applicable regulations articulated by national and international regimes. The right to exercise export controls belongs to the sovereign rights of states to control and regulate cross-border transfer of goods and services (Pezzullo 2014). And it has to be noted that each state performs export controls of space technologies unilaterally. Export control regulations are in fact a reaction to the need to control items – the hardware, the software, or the technology and services leaving their territory – for the reason of security and technology protection.

In accordance with numerous relevant laws and regulations, *export* may be defined as the transfer (note that the term transfer is used for intra-European Union exports, for more details see below) of an item from one country (the country of exportation) to a foreign country (the country of destination) regardless of the method that is used for this transfer. Laws apply based on the nationality of the item. The term *item* may encompass hardware, software, technology, and even know-how. Export is also considered to have occurred if the item leaves the country only temporarily or as an item which is not for sale. Other forms of temporary exports are a wholly owned subsidiary in a foreign country or the transfer of an item with foreign origin from the exporting country to the country of origin (Aubin and Idiart 2011, p. 4). Also, the release of information regarding controlled technology to a foreign entity while the item itself remains on the soil of the country of exportation is considered an export. National export control regimes, such as in the United States (the US export control regime will be further examined below), have a broader scope of application and include deemed exports and the re-transfer inside the same territory of a product to another consignee. Export controls typically focus on strategic items, but some controls on embargoed countries can apply to the export of any item. Further, it is worth noting that more than one set of rules may apply to a single transaction.

The export control systems are often being implemented in the form of licensing authorization processes. In order to estimate whether a license can be granted, several factors are taken into consideration by the relevant administration. First, the goods and the technology submitted to the licensing process have to be examined with regard to their nature. In addition, the end user, the intended end use, and the destination have to be determined. Classification of goods and their placement on such a list derives from their characteristics. Although no consolidated definition of the term *space technology* can be offered, it can be described as a systematic application of engineering and scientific disciplines to the exploration and utilization of outer space (McGraw-Hill Science & Technology Dictionary). Within the export

control laws and regulations, the term often has a very specialized meaning which is applied in the range of the concerned legal or regulatory text. The export control system typically deals not only with the physical item itself but also with the specific information required for the development, production, or use of an item classified commonly as technical data or technical assistance. The term *space technology* refers simultaneously to the physical item as well as to the technical knowledge the item is built upon.

However, the close link between the Fourth Industrial Revolution, also known as Industry 4.0, and new space developments enables the rapidly increasing amount of new space entities to make use of material and technology originally used on Earth in outer space. This kind of technology might not yet fall under the given definitions of *space technology*, which is also varying between the existing export control regimes (see, e.g., EAR and EU Council Regulation 428/2009). In some cases, these items may then be classified as commercial. In the United States, *exempli causa*, these items fall under the jurisdiction of the US Department of Commerce and are designated as EAR99, as the majority of commercial products, which will not require a license to be exported or reexported as long as not exported to an embargoed or sanctioned country, to a party of concern, or in support of a prohibited end use. Nonetheless, the classification of such items has of course to be made on a case-by-case basis and might not be straightforward, where innovative technology is used for the first time in the harsh space environment. Therefore, the expression *technology used in space* might be more suitable in view of the export control classifications than merely *space technology* as the former encompasses a broader range of items than the latter.

The technical characteristics of the space item are a crucial factor in this whole process. If an item intended for export is referenced by a specific export control legal or regulatory text, the prescribed necessary measures in order to obtain a license for its export have to be taken.

The space industry covers a wide range of activities, such as design, construction, and assembling of complete spacecrafts, major subsystems and electronical systems such as earth observation technologies (Rhodes et al. 2015). Consequently, space export-controlled items range from satellites, launching pads to component parts, such as lasers and sensors as well as imagery and high-sensitive data.

Controls are usually conducted on exports of nuclear, chemical, biological, military, or dual-use goods, technology, or services. Virtually, the majority of controlled exports relate to military and dual-use goods and services. *Dual-use goods* are goods that may be used for both nonmilitary and military applications. Dual-use technology can then be described as those products, technologies, and services that can address and serve the needs of the civil and military fields. The military application can be either proven or even potential (Wetter 2009 xv).

As a matter of fact, all space items and technologies, *exempli causa* launch vehicles and satellites, are inherently dual-use since outer space as such is militarily strategic. While some early launch vehicles, such as the launch of Sputnik 1 on the Russian 8K71PS rocket (Konyukhov 2003) or the launch of the first US satellite “Explorer 1” on Army Jupiter-C (Angelo 2006), were converted military ballistic

missiles with almost identical technology which may then have undergone further technological developments, it holds true also for contemporary launch vehicles that are most of the time independent system developments and that they still share many characteristic features and technological bases. Therefore, they are, together with ballistic missiles, classified as delivery mechanisms for weapons of mass destruction. Satellites and their components are modified according to their intended use, which means that they can also be adapted to the requirements imposed by a military purpose. Satellites as well as satellite components are therefore generally categorized as dual-use and may be considered militarily sensitive.

The swings of technology in the aerospace industry, from military to civil applications after the era of the Cold War and back, prove that both areas benefit from a cross-fertilization. Items developed strictly for civil or commercial purposes might still be used for military purposes and vice versa.

The possibility to provide support and strategic advantages to military and intelligence operations is regarded as one of the most important export control characteristics of space technologies. Space technologies have already become an essential element of military and intelligence activities and play an important role in their future planning and structures. These characteristics are not based on the technical qualities of the space technologies but result from their potential use and the benefits they bring.

Therefore, the question that needs to be asked is not how to prevent this inherent dual-use nature, as the solution would be clearly beyond the regulatory or even technical possibilities. The question is what the export control regulations concerning these items should look like (Mineiro 2012, pp. 3–12).

In contrast to export controls, sanctions can be defined as restrictions on transactions with other countries, persons, or entities based on security or policy concerns, which do not necessarily involve items. Instead of the nationality of the item, the nationality of the person involved in the transaction gains central importance in the context of sanctions. Sanctions are not only limited to items, software, or technology and can also encompass financial transactions, related agreements, or services (Wolf, How U.S. Export Controls and Sanctions Affect the Work of the European Space Agency, p. 2.).

---

## International Legal Regimes

Internationally coordinated export controls can contribute to the promotion and preservation of global stability and security. Even though there are no binding multilateral agreements focusing *exclusively* on space technology export control yet, it must be highlighted that a number of multilateral agreements concerning space technology used as weapon delivery systems and documents prohibiting their deployment and operation have been agreed upon and entered into (Gerhard and Creydt 2011, p. 191). Furthermore, some bilateral agreements serving as a basis to exempt respective states from the related licensing process can be found (Mineiro 2012).

The following paragraphs will examine the general international export control regimes and their applicability to space technology. Following that, the impact of the traditional international space law, in a narrower sense, to the space export controls will be investigated.

## The Melee of International Legal Instruments on Export Control

Enhancing international cooperation is a means to maintain peace and international security. “[...] Growing tensions between states wishing to develop their civilian space programs, on one side, and states willing to prevent the traffic of dangerous military items, on the other side, have developed” (Von der Dunk/Tronchetti, *Handbook of Space Law* 2017, p. 360). The dialogue between nations resulted in the establishment of a number of international legal instruments intended to balance the international law principle of protection of peace and international security with the right to legitimate self-defense as well as to development and economic freedom (Achilléas 2007, p. 20). Four separate and almost wholly independent functional regimes compose the current export control system, which supplement the provisions of other binding, multilateral treaties primarily focused on the development and possession of weapon technologies, such as the 1968 Nuclear Non-Proliferation Treaty (NPT) (Treaty on the Non-Proliferation of Nuclear Weapons 1968), the 1972 Biological Weapons Convention (BWC) (Convention on the Prohibition of the Development 1972b), and the 1993 Chemical Weapons Convention (CWC) (Convention on the Prohibition of the Development 1993; Joyner 2004).

The four functional supplier state regimes are:

- The system of the Nuclear Suppliers Group (hereinafter “NSG”, <http://www.nuclearsuppliersgroup.org>), which governs the area of nuclear weapons and materials
- The Wassenaar Arrangement on Export Controls 1996 (hereinafter “Wassenaar Arrangement”), which sets the rules in the context of conventional weapons
- The Australia Group (The Australia Group, <http://www.australiagroup.net/>), which deals with chemical and biological weapons proliferation
- The Missile Technology Control Regime (hereinafter “MTCR” or “The MTCR Guidelines 2012”), which regulates the export of missile and related delivery system technologies

In addition, these regimes are complemented by provisions of the Nuclear Non-Proliferation Treaty (hereinafter “NPT”), the IAEA Comprehensive Safeguards Agreement and Model Additional Protocol (1997), the Zangger Trigger List (1974), the Limited Test Ban Treaty (hereinafter “LTBT”) (Treaty Banning Nuclear Weapon Tests 1963), and the Comprehensive Nuclear-Test-Ban Treaty (hereinafter “CTBT 1996”) regarding nuclear materials and tests; by the Geneva Protocol (1925), the Biological and Toxin Convention (Convention on the Prohibition of the Development 1972), and the Chemical Weapons Convention with regard to chemical and

biological weapons proliferation; by the Hague Code of Conduct (hereinafter “HCoc” or “International Code of Conduct 2002”) concerning ballistic missile proliferation; and by United Nations Register of Conventional Arms (hereinafter “UNROCA 1992”) in the domain of conventional weapons.

By the conclusion of bilateral or multilateral agreements, states coordinate their domestic regulations but generally do not install a specific authority to enforce these obligations. In addition to these partly soft-law instruments, there are only a few specific cases, in which international law imposes direct obligations to control space technology exports. In accordance with Article 39 of the United Nations Charter, the United Nations Security Council is entitled to take actions “to determine the existence of any threat to the peace and shall make recommendations or decide what measures shall be taken in accordance with Artt. 41 and 42, to maintain international peace and security.”

One concrete example is United Nations Security Council Resolution 1540 (UN Doc. S/Res/1540 2004), which was adopted unanimously on 28 April 2004. Security Council Resolution 1540 establishes the obligation under Chap. VII of the UN Charter for all member states of the UN to develop and enforce appropriate legal and regulatory measures against the proliferation of chemical, biological, radiological, and nuclear weapons and their means of delivery, in particular, to prevent the spread of weapons of mass destruction to non-state actors (on an implementation strategy for Resolution 1540, see Heupel 2007). Thus, the UN Security Council may pass on behalf of its 15 member states a resolution, which then establishes the need for member states to adopt and enforce controls over exports insofar as materials and technologies might have the abovementioned impact so that it poses a security threat. This explicit international obligation also impacts the right of states to export space technologies, to the extent that they could be used as a means of delivery for weapons of mass destruction (Mineiro 2012, p. 21). However, so far it never passed a legally binding resolution concerning the export of satellite technology (ibid., p. 20).

In the field of soft-law agreements (on the notion of soft law, see Freeland 2012, with further references), the Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies plays a major role. Numerous space faring nations are parties to it. It is a nonbinding export control agreement aiming at “contributing to regional and international security, by promoting transparency and greater responsibility in transfers of conventional arms and dual-use goods and technologies” (Wassenaar Arrangement, paragraph 1). Certain space and satellite technologies are listed in the categories of sensitive and very sensitive dual-use goods in the annexed List of Dual-Use Goods and Technologies, and their transfer or denial must be therefore duly notified according to the rules set up by the arrangement (Mineiro 2012; Achilléas 2007, p. 53). Following increasing cybersecurity vulnerabilities, the state parties to the Wassenaar Arrangement decided already in December 2017 to include also computer network intrusion software into Category 4 of its Dual-Use List. According to the respective definition the term “Intrusion software” means software specially designed or modified to avoid detection by “monitoring tools,” or to defeat “protective countermeasures,” of a computer or network-capable device, and performing any of the following:

- (a) The extraction of data or information, from a computer or network-capable device, or the modification of system or user data
- (b) The modification of the standard execution path of a program or process in order to allow the execution of externally provided instructions (Wassenaar Arrangement Secretariat 2018, pp. 221–222)

Moreover, launch vehicle space technologies are addressed in two other non-binding instruments – in the Guidelines for Sensitive Missile-Relevant Transfers and the International Code of Conduct against ballistic missile proliferation. The MTCR is a voluntary regime (Jakhu and Wilson 2000, pp. 165–7), applicable to rocket systems, including space launch vehicles and sounding rockets whose transfer could possibly make a contribution to deliver systems other than manned aircraft for weapons of mass destruction. According to the provisions of HCOC, states exporting launch vehicle technology must promote the nonproliferation of ballistic missiles capable of delivering weapons of mass destruction and be vigilant in consideration of assistance to space launch vehicle program in any other country. MTCR and HCOC concern the export of satellite technology only indirectly through the control of items enumerated on their lists. When a satellite technology is used together with these items, these two arrangements have to be taken into consideration and complied with. The MTCR control list contains, e.g., complete rocket systems (suborbital and space launch vehicles) with a payload of 500 kg at a distance of minimum 300 km, its component parts and production facilities, etc. (MTCR, Equipment, Software and Technology Annex 2014, para 1(a); Category I 1.A.1; Category I 1. B.1.). Items listed in Category I underlie a strong presumption of denial (MTCR, Guidelines for Sensitive Missile-relevant Transfer 2003). Category II contains rocket systems with a range of minimum 300 km and dual-use satellite technologies, like flight control systems and hydrazine (*ibid.*, Category II 10.A.1–10. A.3; Category II 4. C.2). An export is authorized if its end use is in line with the MTCR Guidelines and if this is assured by the recipient state (§§ 2,5 MTCR Guidelines; Von der Dunk 2011, p. 194). The MTCR is a nonlegally binding export control regime. To ensure its impact, the HCoC came into force in 2002. In November 2018, 139 states are signatory states of the HCoC, which is a politically binding document (HCoC 2019). It aims certainty and transparency through publication of annual reports.

The above-enumerated international legal regimes apply to export controls of space technology because of its inherent dual-use characteristics and the potential to be used or incorporated in a system of weapons, missiles, or other applications destined for non-peaceful purposes. However, the trade with space technologies falls also under the restrictions posed by specific regimes applying to outer space.

## **The Specificities of the Outer Space Regime**

Outer space as an area beyond national control is subjected to special rules of international public law characterized by principles such as peaceful use and non-

armament (Achilléas 2007, p. 60; for an analysis of outer space law and space security, see Freeland 2012). Article III of the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other celestial bodies (hereinafter “OST” or “Outer Space Treaty 1967”), stipulates that “States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the Moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding.” As a consequence, Article IV paragraph 1 regulates that no objects carrying nuclear weapons or any other kinds of weapons of mass destruction shall be placed in orbit around the Earth and no such weapons shall be installed on celestial bodies or stationed in outer space in any other manner. This Article has been considered as one of the first provisions on arms control (Schrogl and Neumann 2010). As may be observed, placing of other than nuclear weapons and weapons of mass destruction in outer space is not expressly excluded; also, a transfer of weapons is not explicitly prohibited. With regard to the fact that the Earth’s orbits are of an immense strategic and also military value, this loophole may serve states future interests.

According to Article IV paragraph 2, the moon and other celestial bodies shall be used “exclusively for peaceful purposes.” Since the Outer Space Treaty itself does not provide a definition of the term “peaceful,” its interpretation has over the years given rise to much debate centered on the question as to whether it is to be understood as meaning “nonmilitary” or “nonaggressive,” with the latter meaning seeming to have gained general acceptance (e.g., Markoff 1967; Hobe and Hedman 2010). Irrespective of the meaning attributed to the term in other provisions of the Outer Space Treaty, its combination with the term “exclusively” in Article IV paragraph 2 leads to an all-embracing prohibition of military use of the moon and other celestial bodies even if of nonaggressive nature (Schrogl and Neumann 2010). This is supported by a parallel to other international treaties and legal instruments: Article I of the Antarctic Treaty providing “for peaceful purposes only” is commonly understood as complete demilitarization of Antarctica. In addition, the United Nations Convention for the Law of the Seas (hereinafter “UNCLOS”) distinguishes between “exclusively for peaceful purposes,” referring to nonmilitary use of the seabed (Art. 141) and “shall be reserved for peaceful purposes” (Art. 88), allowing for military but nonaggressive use.

The establishment of military bases, installations and fortifications, the testing of any type of weapons, and the conduct of military maneuvers on celestial bodies shall be forbidden. Only scientific research and peaceful exploration may be conducted, also by military personnel.

Article III OST provides that “States Parties to the Treaty shall carry on activities in the exploration and use of outer space, including the Moon and other celestial bodies, in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding.”

Accordingly, it may be concluded that all disarmament and nonproliferation treaties that are part of international law are also applicable to activities carried out

in outer space. This is further supported by Article 38 (1) of the Statute of ICJ; the recognized source of international law includes apart from international conventions also international custom, as evidence of a general practice accepted as law and the general principles of law recognized by civilized nations.

---

## National and Regional Legal Regimes

In order to provide an overview of the complexities related to the legal export control regimes of space technologies, the following sub-chapters look at two prominent examples of national and regional legal regimes: the US regime on the one hand and the European Union system on the other. Following that, a sub-chapter sheds light on the additional particularities of dealing with export control issues in an international organization dedicated to the promotion of cooperation among its member states in space research and technology and their space applications, the European Space Agency (hereinafter “ESA”).

### The Export Control Regime of the United States

One unique characteristic of the US export control regime is the extraterritorial jurisdiction it establishes over US goods and technology. US export controls apply also when these items or technologies are located outside the territory of the United States, based on the fact that these are of US-origin or contain significant US content (for further details, Gerhard and Creydt 2011). This extraterritorial application of jurisdiction, which has given rise to criticism and debate over the years (e.g., Ress 2000; Clement 1988), is, however, a fact of law (see for more details Little et al.) and has a great impact not just on US American firms but on exporters all around the world since any foreign company seeking to re-export a product of US origin or with a certain percentage of US technology (details can be found in Part 734.4 EAR) will always have to comply with the applicable US regulations, regardless of whether they export from US territory or from any other place in the world. More precisely, § 734.4 and Supplement No. 2 to part 734 Export Administration Regulation (hereinafter “EAR”) set out the scope of application of the US *De minimis* Rules and Guidelines. It applies if non-US-made commodity or software incorporates or is bundled with controlled US-origin commodities or software or in case that non-US-made technology is commingled with or drawn from controlled US-origin technology. If the abovementioned circumstances apply, the non-US-made item is subject to the EAR if the US- origin-controlled content exceeds a dedicated percentage based on destination.

In the *Nottebohm Case* (Liechtenstein v. Guatemala, I.C.J. 4 1955), the extraterritorial applicability of US export controls was fiercely discussed and finally considered to be in accordance with international law through the channel of national sovereignty under compliance with the “genuine link requirement.” Failure to comply may give rise to prosecution, blacklisting, or other forms of punishment. It



is worth pointing out in this context that re-export has been elaborated as follows: “In addition, for purposes of *satellites* controlled by the Department of Commerce, the term “re-export” also includes the *transfer of registration of a satellite or operational control* over a satellite from a party resident in one country to a party resident in one country to a another country” (Part 77. Part 772 EAR). From a US perspective and understanding, there is no general freedom or right to export goods. Rather, an export license is considered to be a privilege which can be revoked in case of noncompliance with applicable regulations. Article I Sect.8 US Constitution authorizes the US congress to enact norms to ensure security and foreign trade. The United States is involved in international agreements, e.g., WA and MTCR, and implements them into national law (von der Dunk and Tronchetti 2017, p. 364).

Despite their importance for national security and for the overall economy, the US regime of export regulations has not been consolidated into a single and unified text. Instead, there are different rules applied by different departments depending on the individual item and recipient in question:

- *Dual-use goods*, i.e., goods that may be used for both nonmilitary and military applications, are regulated by the Export Administration Regulations (EAR).
- *Military goods* are governed by the International Traffic in Arms Regulations (ITAR).
- Finally, the Office of Foreign Assets Control Regulations (OFAC) relates to *particular countries, organizations, and persons* for the protection of national security interests.

With regard to OFAC, it must be pointed out that, unlike the EAR and ITAR, the main focus of these regulations is not on particular items and services but on targeted countries and end users: OFAC administers, upholds, and enforces economic trade sanctions based on US foreign policy and national security goals against targeted foreign states, organizations, and individuals. OFAC derives its authority from a variety of US federal laws regarding economic sanctions. The effect on the American space industry of these regulations is, however, only marginal given that the targeted countries are not important trading partners in the field of space technology.

Further, on 30 June 2017, US President Trump signed the Executive Order on Reviving the National Space Council. The Council’s recommendations to the US President for regulatory reforms and other actions aim to “unleash the economic potential of the U.S. commercial space industry” (Office of Space Commerce 2019). The Aerospace Industries Association (AIA) announced “While the U.S. experienced the third largest trade deficit on record, our industry generated \$143 billion in exports and a positive trade balance of \$86 billion, effectively reducing the U.S. trade deficit by 10 percent” (Aerospace Industries Association (AIA) 2018, p. 1.).

### **Dual-Use Goods: The Export Administration Regulations (EAR)**

The US Department of Commerce is empowered to administer and to enforce rules for the export of dual-use items under the Export Administration Act of 1979 (Export Administration Act of 1979). More specifically, its Bureau of

Industry and Security is charged with the development, implementation, and interpretation of US export control policy for dual-use items under the EAR. § 730.5 EAR refers to a broad meaning of the term “export,” which applies to transactions outside of the United States or to activities other than exports. For instance, re-exports are defined by § 734.2 (b) and include in regard of space items also the transfer of registrations or monitoring/control over satellites (Part 772.1 EAR), which plays a decisive role in the monitoring of space debris. In addition, EAR applies to deemed re-exports, which are defined as releases of technology or software source code subject to EAR, within a state outside the United States, to persons who are not citizens or lawful permanent residents of that state (third-country nationals). Exceptions are imposed for the releases to nationals of certain countries (A:5 Country Group) and to certain bona fide regular and permanent employees.

Moreover, EAR encompasses in-country transfers of commodities, software, and technology that remain “subject to the EAR” once outside of the United States. Such items include:

- US-origin items, wherever located, if in their original form
- Non-US items incorporating more than de minimis amount of US-origin-controlled content
- Non-US items that are direct product of certain US-origin technology or software

The EAR establishes a number of general prohibitions (Part 736.2 EAR) relating to certain exports, re-exports, and other conduct, subject to the scope of the EAR, which necessitate a license from the Bureau of Industry and Security or the qualification for a license exception. Facts that determine the applicability of the general prohibitions are:

- The classification of the item on the Commerce Control List
- The country of ultimate destination for an export or re-export
- The ultimate end user
- The ultimate end use
- Conduct such as contracting, financing, and freight forwarding in support of a proliferation project

The relevant details are provided in accompanying lists and schedules. It is interesting to note that the otherwise existing possibility to obtain a license exception is specifically excluded for a number of items, among which feature certain “space-qualified items” (Part 740.2(a)).

Once established that an envisaged export activity does not fall under a general prohibition, the exporter needs to examine the specific license requirements, if any. This examination is accomplished by means of the CCL and the Country Chart, as well as the established reason for the control of the item (Gerhard and Creydt 2011, p. 198). The space relevant categories are Category 6, dealing with lasers and sensors and Category 9, which is listing propulsion systems, space vehicles and

related equipment. The Commerce Control List (hereinafter “CCL”) includes dual-use items such as listed on the WA and MTCR list and also items under the “catch-all clause” (U.S. Department of State, A Resource on Strategic Trade Management and Export Controls 2016). Criminal sanctions, in addition to administrative and civil penalties, can be imposed where the EAR regulations have been violated (Part 764.3 EAR).

As a result of the 2013/2014 Export Control Reform, numerous items, such as transitioned military items (600 series) and transitioned spacecraft items (ECCNs 9A515), were moved from ITAR to the EAR. As of end 2014, the majority of commercial spacecraft items were moved from ITAR to EAR, where they are classified under:

- ECCN 9A515: Commercial communication satellites and spacecraft including lower-performing remote sensing satellites, planetary rovers and (inter-)planetary probes, related systems for these and parts/components of satellite bus, and payloads not listed on the USML
- ECCN 9A004: International Space Station (hereinafter “ISS”), James Webb Space Telescope, and parts or components thereof.

The revised United States Munitions List (hereinafter “USML”) Category XV covers now satellites and spacecraft providing unique military and intelligence functions, human-rated habitats, and certain ground control equipment and parts/components. The latter includes 18 specific technologies critical to military functions, any payload performing the military functions described above, and US DoD funded payloads.

Restrictions on certain “military end uses” in the People’s Republic of China and Russia or “military end users” in Russia are imposed. Exceptions are defined in EAR 744.21 for export, re-exports, transfers, and launch within Russia for the ISS. Stricter requirements for military end users in the People’s Republic of China are expected in May 2019.

License exceptions can result from the *de minimis* rule, which is based on:

- The percentage, by value, of US-origin-controlled content in a foreign-made item
- The intended destination of the re-export or deemed re-export
- *De minimis* percentage: 0% threshold for 9x515 (The 9x515 Export Control Classification Number (hereinafter “ECCN”) describes “spacecraft,” related items, and some radiation-hardened microelectronic circuits that were previously subject to the International Traffic in Arms Regulations (hereinafter “ITAR”)) to China, 10% threshold for Iran, North Korea, Syria, and Sudan, as well as 25% threshold applicable to all other countries.

Secondly, it can result from a Strategic Trade Authorization (hereinafter “STA”), requiring a prior consignee statement for transfers and re-exports in the A:5 country group (37 US partners and allies including all ESA member states). Lastly, license exemptions apply for US government programs (hereinafter “GOV”).

### **Military Goods: The International Traffic in Arms Regulations**

“[...] For everyone active in the space sector, knowledge about how to deal with International Traffic in Arms Regulations (hereinafter “ITAR”) is absolutely necessary” (Gerhard and Creydt 2011, p. 203; current version [http://pmddtc.state.gov/regulations\\_laws/itar\\_official.html](http://pmddtc.state.gov/regulations_laws/itar_official.html)). ITAR governs the export, re-export, re-transfer, and temporary import of defense items and services. Under the Arms Export Control Act of 1976, the State Department has the delegated power to control, enforce, and administrate the regulations. These defense articles and services are listed in the United States Munitions List (hereinafter “USML”) (Part 121 ITAR). USML categories of particular interest in the context of space activities are:

- Category XV: Satellites and Spacecraft, providing unique military and intelligence functions
- Category IV: Launch Vehicle, including any interface between any spacecraft and a launch vehicle
- Category XII: Fore Control. Laser, Imaging and Guidance Equipment, such as Global Navigation Satellite System (hereinafter “GNSS”) receiving equipment exceeding the “CoCom rule”
- Category XIII: Materials and Miscellaneous Articles

Following the passing of the Strom Thurmond National Defense Authorization Act for fiscal year 1999 (Public Law 105–261 1998), the export control competence concerning commercial satellites was shifted from the Department of Commerce to the Department of State following concerns about the proliferation of sensitive satellite technology (for the background and details, van Fenema 1999, p. 332). Exports under the ITAR are broadly defined (Annex 5 reflects a detailed scope of application), also covering:

- Exports of defense articles outside the United States.
- Transfer of registration, control, or ownership to a foreign person of any aircraft, vessel, or satellite covered by the USML, whether in the United States or abroad.
- Disclosing/transferring in the United States of any defense article to foreign government and disclosing technical data to a foreign person
- Performing a defense service for foreign person

ITAR consists of 11 parts (§§120–130) and aims to enforce the Arms Export Control Act (hereinafter “AECA”). Administrating body of the AECA is primarily the Department of State under the Directorate of Defense Trade Controls (hereinafter “DDTC”).

An authorization is the prerequisite for conducting an export, re-export, or transfer of an ITAR-controlled item, regardless of its destination. Different license requirements exist for the permanent or the temporary export of any defense article or technical data (§§ 123 and 125 ITAR). The performance of defense services also requires the prior approval by the Directorate of Defense Trade Controls of the State

Department, which requires the conclusion of specific agreements between the performer of such services and the respective international partner (§§ 124.1 ITAR). Conclusively, authorization can be obtained in form of a license (DSP-5, DSP-83, DSP-73) or an agreement (Technical Assistance Agreement (hereinafter “TAA”) (§ 120.22 defines the Technical Assistance Agreement as an agreement for the performance of a defense service and/or the disclosure of technical data (including the assembly of defense articles, providing that production rights or manufacturing know-how are not conveyed, which are to be covered by a MLA), Manufacturing License Agreement (hereinafter “MLA”) (§ 120.21 defines a Manufacturing license agreement as an agreement granted by a US national to a foreign person to manufacture defense articles abroad, which involve either the export of technical data (§120.10 ITAR), defense articles, the performance of a defense service, or the use by the foreign person of technical data or defense articles previously exported by the US national (§124 ITAR))).

The “see-through” rule applies to commodities, software, and technical data. According to this rule, any non-US-made item incorporating US-origin ITAR content will require DDTC approval to re-transfer the ITAR content, regardless of the type of content or destination. Compared to the EAR, ITAR “sees through” the item and continues to control the original ITAR content. Further, there is no *de minimis* threshold in the ITAR. However, some ITAR-controlled items are exempted from the “see-through” rule when incorporated into an EAR controlled system, e.g., USML spacecraft (Category XV) items.

There are only a few exemptions from ITAR authorization requirements, such as the Defense Trade Cooperation Treaties with Australia and the United Kingdom for certain governmental end users (Long 2013, p. 58 ff.). In addition, ITAR contains exemptions for transfers to regular employees (including loan-employment contractors) from NATO and EU member states, Switzerland, Australia, Japan, and New Zealand. It follows that this exemption applies to all ESA member states. A transfer of items or services to dual/third-country nationals outside these countries can be made in the framework of:

- Foreign vetting
- DDTC vetting

The ITAR regulations have been criticized as too cumbersome, complex, and time-consuming (e.g., Abbey and Lane 2009), which in turn is said to have led to a competitive disadvantage for the US space industry and a decline of exports, as competitors around the globe started to invest in the non-dependence in certain fields of technology (see also Landry 2010). However, with Space Policy Directive – 2 “Streamlining Regulations on Commercial Use of Space,” which was signed by President Donald J. Trump in May 2018, the White House is eager to ensure the promotion of economic growth and the minimization of uncertainties for taxpayers, investors, and private industry while protecting national security, public safety, and foreign policy interests.

The overall objective is the encouragement of American leadership in space commerce (the White House. President Donald J. Trump is Reforming and Modernizing American Commercial Space Policy 2018).

Space Policy Directive 2 addresses five areas:

1. Commercial launch and licensing
2. Commercial remote sensing
3. Creation of an Office of Space Commerce within the Department of Commerce
4. Radio frequency spectrum management
5. Export licensing

The latter requests the National Space Council to review of export licensing affecting commercial space flight as well as commercial remote sensing activities with strict consideration of US commercial space policy objectives. As a result, the NASA Advisory Council Regulatory and Policy Committee issued recommendations to relieve the Lunar Gateway from such licensing restrictions as are applicable to the ISS (NASA Advisory Council Regulatory and Policy Committee Observations, Findings, and Recommendations of 12 October 2018).

In October 2018, the US State Department issued minor ITAR revisions, including two space relevant changes. As result of a previous revision conducted by the Department of Commerce's Bureau of Industry and Security (BIS), the State Department added a note clarifying that the rocket engine controls in Category IV(d) of the USML do not apply to satellite and spacecraft thrusters. Such thrusters fall under USML Category XV(e)(12) or ECCN 9A515 of the CCL. Further, the ITAR update also amended the definition of spacecraft-related defense services in USML Category XV(f), but without changing the actual scope of the controls (Office of Space Commerce. ITAR Clarification on Satellite Thrusters 2018). After the recent update of the USML, Category XV now includes letter (f) "the furnishing of assistance (including training) to a foreign person in the launch failure analysis of a satellite or spacecraft, regardless of the jurisdiction, ownership, or origin of the satellite of spacecraft, or whether technical data is used."

## **Export Regulations of the European Union**

The European Union (EU) has for many years played a leading role in arms export control, both regionally and internationally. Nowadays, export control regulations on dual-use goods and defense equipment have been harmonized within the EU under a common regime. Similar to the US approach, products are categorized into either dual-use goods or military products. However, unlike to the situation in the United States, none of the regulations or national laws has extraterritorial effect on third countries outside the EU.

However, the categorization of items in dual-use and defense equipment caused conflicts of competences. EU competences are laid down in the EU treaties. Article 3 (1.e) of the Treaty on the Functioning of the European Union (hereinafter "TFEU")

provides for the exclusive competence of the EU over Common Commercial Policy (hereinafter “CCP”). Article 207 defines the scope of CCP, which can be summarized as unified basis for trade affairs, e.g., liberalization and export control. At the same time, Art. 4(1) of the Treaty of the European Union (hereinafter “TEU”) sets out the exclusive member state authority over national security matters since member states prefer to exercise their sovereignty in this area. Moreover, Art. 346 of the Lisbon Treaty provides for member state’s sovereignty on “public security.”

Prior to 2009, national rules regulating the transfer of defense equipment did not necessarily distinguish between exports to third countries and transfers between EU member states.

Space activities are business activities. However, they cover the transfer of dual-use items, which has to be assigned to the objectives of national security and foreign policy as it refers to nonproliferation. Accordingly, the EU set up a Council Regulation (Council Regulation (EC) No. 3381/94, OJ L 367/1) based on CCP and a Council Decision (Council Decision 94/942/CFSP, OJ L 367/8) based on the Common Foreign and Security Policy (hereinafter “CFSP”) to create a common export control regime for dual-use items. The underlying competence of CCP was defined by the European Court of Justice (hereinafter “ECJ”), resulting in the exclusive competence over EU external trade relations (Opinion of the Court of 11 November 1975 given pursuant to Article 228 of the EEC Treaty – Avis 1/75). Thus, according to Art. 2(1) TFEU only the EU might legislate and adopt legally binding acts in CCP.

The currently applicable Council Regulation (EC) No. 428/2009 (hereinafter referred to as EU Dual-Use Regulation) was established after the ECJ decided to assign dual-use exports to the scope of the CCP and, by doing so, to the exclusive EU competence (Fritz Werner Industrie-Ausrüstungen GmbH v Federal Republic of Germany; Criminal proceedings against Leifer and others). Council Regulation 428/2009 of May 2009 (Council Regulation No. 428/2009 of 5 May 2009 setting up a community regime for the control of exports, transfer, brokering, and transit of dual-use items, OJ L 134) governs the export of dual-use goods from a country within the EU to a third country. In addition, the export of military goods and defense-related products is regulated by Directive 2009/43 (<http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri%40OJ:L:2009:146:FULL:EN:PDF>), the European Union Code of Conduct on Arms and Exports, and the Common Military List of the European Union. Under the regime established by Directive 2009/43, member states can issue general licenses for those exports throughout the EU where the risk of re-exportation to foreign countries is under control. At the same time, the nation states retain their discretion to determine the eligibility of products for the different types of license and to fix their terms and conditions. In 2008, the European Council also agreed on the Common Position 2008/944/CFSP defining common rules governing control of export of military technology and equipment to *third* countries. It should be noted, however, that the impact of these rules on the European space industry is not particularly important, since most space-related items are considered dual-use and not military items. There are also council regulations restricting the export against specific countries, e.g.,

Myanmar (Council Decision 2010/232/CFSP). Moreover, Council Regulation (EU) No 833/2014 of 31 July 2014 introduces certain restrictive measures as applicable for exports of items and services under Council Regulation (EC) No 428/2009 and on certain service related to the supply of arms and military equipment, if an embargo on such goods is applied by the member states. However, the prohibition should not affect the exports of dual-use goods and technology, including for aeronautics and for the space industry, for nonmilitary use, or for a nonmilitary end user (Council Regulation (EU) No 833/2014, pp. 1–11). The aim of this harmonization is to promote European and international security as well as to allow for comparable conditions for all economic entities within the EU's common market. Despite this development, some differences do, however, remain among EU member states with regard to export control licensing (Gerhard and Creydt 2011, p. 210).

### Dual-Use Items

§12 of the preamble of Council Regulation 428/2009 provides that “[...] Member States retain the right to carry out controls on transfers of certain dual-use items within the Community in order to safeguard public policy or public security.” As a consequence, member states implement the Regulation by issuing licenses and enforcing export control in accordance with Art. 9 of this Regulation (Art. 9, (EC) No.428/2009.; Wetter 2009, p. 49). It was adopted as a single document abandoning the “cross-pillar” approach (Aubin and Idiart 2011, p. 109). Free trade of dual-use items within the EU is one of the general principles (§ 4 Preamble, European Union Regulation (EC) 428/2009). The Council Regulation 428/2009 establishes a common community export licensing system, a common control list, and a common export authorization. Dual-use items which require a license to be exported from the EU are listed in Annex I. Most space assets are regarded as dual-use items under Annex I: Category 9, aerospace and propulsion, lists the different systems, equipment, components, materials, software, and technology subject to the regulation. Authorizations, which are valid throughout the community, are granted by the competent authorities of the member state where the exporter is established. Pursuant to Article 22.1 of Regulation 428/2009, dual-use goods items in Annex IV of the regulation are considered to be particularly sensitive and require a license even to be traded *within* the European market. This procedure, which concerns also quite a number of space-related items, constitutes an exception to the principle of free movements of goods (Wetter 2009, p. 54). It is interesting to note that Annex IV establishes some explicit exemptions (OJL 134, p. 264) and as such does not control the following items of the MTCR technology:

1. That are transferred on the basis of orders pursuant to a contractual relationship placed by ESA or that are transferred by ESA to accomplish its official tasks
2. That are transferred on the basis of orders pursuant to a contractual relationship placed by a member state's national space organization or that are transferred by it to accomplish its official tasks



3. That are transferred on the basis of orders pursuant to a contractual relationship placed in connection with a community space launch development and production program signed by two or more European governments
4. That are transferred to a state-controlled space launching site in the territory of a member state, unless that member state controls such transfers within the terms of this regulation

On 10 October 2018, Commission Delegated Regulation (EU) 2018/1922 amended Council Regulation 428/2009. This delegated regulation revises the EU dual-use list in Annex I in accordance with the decisions taken within the framework of the international nonproliferation regimes and export control arrangements in 2017. The majority of changes results from amendments of the 2017 Plenary of the Wassenaar Agreement. Space relevant among them is the increase of controls for ground-based spacecraft control equipment (9A004). In addition, Section 4E001 now covers new decontrol for technology for “vulnerability disclosure” and “cyber incident response.”

The Missile Technology Control Regime agreed in 2017 to amend the control on satellite navigation systems (7A105) to include regional and global systems.

Another renewal in European Union Export Controls is the EU foreign investment screening regulation, which entered into force on 10 April 2019. It is based on a proposal scheduled by the European Commission in September 2017 and intends to ensure Europe’s security and policy order in relation to foreign direct investment within the EU.

The EU is the main destination for foreign direct investment in the world with an amount of € 6.295 billion at the end of 2017. The new framework aims to create a cooperation mechanism between member states and EU Commission to enable exchange on the matter and “[. . .]allow the Commission to issue opinions when an investment poses a threat to the security or public order of more than one Member State, or when an investment could undermine a project or programme of interest to the whole EU, such as Horizon 2020 or Galileo[. . .]” (European Commission. EU foreign investment screening regulation enters into force 2019). Moreover, it intends to foster international cooperation on investment screening and to establish requirements for national screening mechanisms.

---

## **The Export Control Regulations of the European Space Agency**

The European Space Agency (ESA) is an international organization created by the Convention for the establishment of a European Space Agency, which was opened for signature in Paris on 30 May 1975 and entered into force on 30 October 1980. According to Article II ESA Convention, its member states entrusted ESA “[. . .] to provide for and to promote, for exclusively peaceful purposes, cooperation among European States in space research and technology and their space applications, with a view to their being used for scientific purposes and for operational space applications systems [. . .]”.

While Article VI of Annex I to the ESA Convention provides that “Goods imported or exported by the Agency or on its behalf, and strictly necessary for the exercise of its official activities, shall be exempt from all import and export duties and taxes and from all import or export prohibitions and restrictions,” in drawing up the Convention, ESA member states also paid heed to the potentially highly sensitive nature of the technology developed and introduced with Article XI.5(j) of the ESA Convention, a starting point for ESA’s own rules and procedures with regard to export control issues.

It provides that:

The ESA Council shall adopt, by a two-thirds majority of all Member States, rules under which authorisation will be given, bearing in mind the peaceful purposes of ESA, for the transfer outside the territories of the Member States of technology and products developed under the activities of ESA or with its assistance.

These rules supplement the regular national export control procedures. Exports remain in their essence governed by national laws and regulations, given their foreign policy and security implications, even in the case of an export of technologies or products developed under the activities or with the help of ESA.

This basic provision of Article XI.5(j) of the ESA Convention is implemented by Chap. IV of the ESA Rules on Information, Data, and Intellectual Property, adopted by the ESA Council on 19 December 2001 (rules), ESA/CCLV/Res. 4 (final). These rules are intended to ensure close liaison between the agency and the national export control authorities of the member states. In line with general ESA policy considerations, the rules contribute to promoting the maximum exploitation of ownership rights by drawing a clear distinction between technology and products that are owned by ESA, on the one hand, and those which are owned by contractors of the agency, on the other hand: the transfer of technology or products owned by ESA necessitates the *authorization* by the Agency Technology and Product Transfer Board (hereinafter “ATB”), whereas the transfer of technology or products owned by contractors only needs to be subject of a *recommendation* by the ATB.

The ATB’s authorization or recommendation, which is – again – not a substitute for the national-level authorization process but rather an additional procedure, is not necessary when the transfer of technology or products is made pursuant to a cooperative agreement between ESA and a government agency of the country of destination. In such case, it is assumed that the ESA Council, when approving the cooperative agreement, has given an overall authorization for the transfer of data and goods in accordance with the relevant provisions of the agreement.

In a first instance, the ATB functions according to a written procedure: when the technology or products are owned by ESA, the transfer proposal is *rejected* when one-third or more of all member states have communicated their opposition. When the technology or products are owned by a contractor, a transfer is *not recommended* where one-third or more of all ATB delegations have communicated their opposition. If, however, within a given time frame, one or more ATB delegations request a meeting to discuss the matter, the ATB Chair convenes such a meeting. The decision shall then be taken at that meeting, with a two-thirds majority of all ATB delegations

present (resolution amending the terms of reference for the Agency Technology and Product Transfer Board (ATB), adopted on 11 October 2006, ESA/C/CLXXXIX/Res. 2 (Final), which amends the terms of reference adopted by the resolution on the creation of an Agency Technology and Product Transfer Board, ESA/C/CLXVII/Res. 1 (Final), adopted on 8 October 2003).

In considering its authorizations and recommendations, the ATB takes into account several factors, such as:

- That the purpose of the Agency is to provide for and to promote, for exclusively peaceful purposes, cooperation among European states in space research and technology and their space applications
- The competitive position of the member states industrial entities as a whole and the competitive edge and technical lead for technology and products
- The relevant provisions of the member states export control laws and regulations
- The requirement for timely implementation of the Agency's programs and activities
- The requirement for restrictions on re-export and/or the existence of any relevant technology transfer agreements

ESA's rules do not prejudice the fact that export control is a national competence, governed by the national laws and regulations of the member states and, in numerous instances, subject to those international agreements by which the member states are bound. This implies also that a certain technology or product that has been developed under an ESA program may still need to be submitted to the regular national export control procedure in case it is planned to be used in another ESA program by another member state than the member state of the originator. In line with that, Article XXIII of Annex I to the Convention provides, "Each Member State shall retain the right to take all precautionary measures in the interests of its security."

In the particular case of an ESA project incorporating US-origin content, software, or information or in when ESA is partnering with NASA and US companies, complying with US export controls is of utmost importance. As a result, ESA may be restricted in its ability to:

- Re-transfer or re-export that US-origin content to other entities within European countries or from one country to another
- Share the US-origin information or software with certain employees, contractors, or other individuals within ESA
- Re-transfer or re-export ESA prototypes or finished products to other countries, including for launch

---

## Conclusions

"Space has a security dimension and security has a space dimension" (European Commission White Paper 2003, p. 17). Space export controls are conducted in an extremely complex set of rules and regulations governing the trade in space items,

items that are not only used in an ultra-hazardous environment but are also dual-use by nature. As the evolution of space activities is closely linked to scientific and technological innovations, new developments in these sectors need to be taken into account. The presented revisions to the existing export control regimes reflect the growing awareness of technological developments and areas of vulnerability.

In addition, with the ever-increasing interest in space activities and related growing participation, diverse policy objectives and varying policy considerations play a central role in this global environment that is evolving at an ever-increasing pace. The diverging interests of governments, international organizations, space agencies, and private actors need to be investigated and balanced while taking into consideration that the international trade in technology is influenced by the interplay between commercial interests, foreign policy objectives, and national security considerations in respect to the proliferation of sensitive technologies. The different approaches and national concepts to regulate the trading in space items provide therefore a characteristic exemplification of how individual nations balance these different and conflicting interests – what degree of importance they attach in their system of political values to one in relation to the others.

---

## References

- Abbey G, Lane N (2009) United States space policy: challenges and opportunities gone astray. American Academy of Arts and Sciences. <http://carnegie.org/fileadmin/Media/Publications/PDF/spaceUS.pdf>
- Achilléas P (2007) International regimes. In: Aubin Y, Idiart A (eds) Export control law and regulations handbook – a practical guide to military and dual-use goods trade restrictions and compliance. Kluwer Law International BV, p 20
- Aerospace Industries Association (AIA) (2018) Facts & figures U.S. Aerospace & Defense. [http://www.aia-aerospace.org/wp-content/uploads/2018/07/2018\\_-\\_Annual-Report\\_Web.pdf](http://www.aia-aerospace.org/wp-content/uploads/2018/07/2018_-_Annual-Report_Web.pdf)
- Angelo JA Jr (2006) Encyclopedia of space and astronomy. Facts on File Inc, New York
- Art 9 (2) Council Regulation No. 428/2009
- ASD Europe (2018) The State of the European Space Industry in 2017. Available at <https://eurospace.org/wp-content/uploads/2018/06/eurospace-facts-and-figures-2018-press-release-final.pdf>. Accessed 30 Apr 2019
- Aubin Y, Idiart A (2011) Export control law and regulations handbook – a practical guide to military and dual-use goods trade restrictions and compliance. Kluwer Law International BV Brussels, 10 April 2019 (2019). [http://europa.eu/rapid/press-release\\_IP-19-2088\\_en.htm](http://europa.eu/rapid/press-release_IP-19-2088_en.htm)
- Clement I (1988) American export controls and extraterritoriality. School of law LLM Theses and Essays, Paper 121, University of Georgia
- Comprehensive Nuclear-Test-Ban Treaty, Adopted by the United Nations General Assembly on 10 Sept 1996, but it has not entered into force as of Aug 2012, published in A/50/1027
- Convention on the Prohibition of the Development (1972a) Production and stockpiling of bacteriological (biological) and toxin weapons and on their destruction, signed on 10 April 1972, entered into force on 26 March 1975. <http://www.opbw.org/convention/conv.html>. Accessed 20 Aug 2012
- Convention on the Prohibition of the Development (1972b) Production and stockpiling of bacteriological (biological) and toxin weapons and on their destruction, signed on 10 April 1972, entered into force on 26 March 1975. Available at <http://www.unog.ch/80256EDD006B8954/>

- ([http://Assets/C4048678A93B6934C1257188004848D0/\\$file/BWC-text-English.pdf](http://Assets/C4048678A93B6934C1257188004848D0/$file/BWC-text-English.pdf). Accessed 24 Aug 2012
- Convention on the Prohibition of the Development, Production, stockpiling and use of chemical weapons and on their destruction, opened for signature on 13 Jan 1993, entered into force on 29 Apr 1997, A/RES/47/3
- Council Decision 94/942/CFSP of 19 December 1994 on the joint action adopted by the Council on the basis of Article J.3 of the Treaty on European Union concerning the control of exports of dual-use goods, OJ L 367/8. Available at <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=OJ:L:1994:367:FULL&from=DE>
- Council Decision 2010/232/CFSP (OJ L 105, 27 Apr 2010, p 22). Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2010:105:0022:0108:EN:PDF>
- Council Regulation (EC) No. 3381/94, of 19 December 1994 setting up a Community regime for the control of exports of dual-use goods, OJ L 367/1. Available at <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31994R3381>
- Council Regulation (EU) No 833/2014 of 31 July 2014 concerning restrictive measures in view of Russia's actions destabilising the situation in Ukraine OJ L 229, pp 1–11. Available at <https://eur-lex.europa.eu/legal-content/GA/TXT/?uri=CELEX:32014R0833>
- Council Regulation No. 428/2009 of 5 May 2009 setting up a community regime for the control of exports, transfer, brokering, and transit of dual-use items, OJ L 134. Available at [http://trade.ec.europa.eu/doclib/docs/2009/june/tradoc\\_143390.pdf](http://trade.ec.europa.eu/doclib/docs/2009/june/tradoc_143390.pdf)
- Directive 2009/44/EC of the European Parliament and of the Council of 6 May 2009 simplifying terms and conditions of transfers of defense-related products within the community, OJ L 146/1. <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:146:FULL:EN:PDF>
- ECJ on 17th October 1995, Case C-70/94 Fritz Werner Industrie-Ausrüstungen GmbH v Federal Republic of Germany [1995] ECR I-03189 [cited as: Fritz Werner Industrie-Ausrüstungen GmbH v Federal Republic of Germany].
- ESA Space Economy. Available online at: [https://www.esa.int/About\\_Us/Business\\_with\\_ESA/GSEF/Space\\_Economy/\(print\)](https://www.esa.int/About_Us/Business_with_ESA/GSEF/Space_Economy/(print)). Accessed 07 Feb 2019
- European Commission (2003) White paper. Space: a new European frontier for an expanding Union. An action plan for implementing the European Space policy [http://www.dlr.de/rd/en/Portaldata/28/Resources/dokumente/WhitePaper\\_en.pdf](http://www.dlr.de/rd/en/Portaldata/28/Resources/dokumente/WhitePaper_en.pdf)
- European Commission. EU foreign investment screening regulation enters into force
- Freeland S (2012) The role of “soft law” in public international law and its relevance to the international legal regulation of outer space. In: Marboe I (ed) *Soft law in outer space, the function of non-binding norms in international space law*. Böhlau, Wien, p 9
- Gerhard M, Creydt M (2011) Safeguarding national security and Foreign policy interests – aspects of export control of space material and technology and remote sensing activities in outer space. In: von der Dunk FG (ed) *National space legislation in Europe, issues of authorisation of private space activities in the light of developments in European Space Cooperation*. Brill, Leiden, pp 189–224
- Guidelines for Sensitive Missile-Relevant Transfers, adopted 16 Apr 1987, 26 ILM 599
- Hertzfeld H, Jones R (2011) International aspects of technology controls. In: Brünner C, Soucek A (eds) *Outer space in society, politics and law*. Springer, Vienna
- Heupel M (2007) Implementing UN Security Council Resolution 1540: a division of labour strategy, Carnegie papers, nonproliferation program, number 87
- Hobe S, Hedman N (2010) On the preamble of the 1967 Outer Space Treaty. In: Hobe S, Schmidt-T B, Schrogl K.-U (eds) *Cologne Commentary on Space Law, Vol 1. Outer Space Treaty*, Carl Heymanns Verlag, Köln
- IAEA Comprehensive Safeguards Agreement and Model Additional Protocol, entered into force on 12 Sept 1997, published in INFCIRC/540
- International Code of Conduct against ballistic missile proliferation established on 25 Nov 2002. Available at <http://www.unhcr.org/refworld/docid/3de488204.html>. Accessed 19 Aug 2012

- International Court of Justice on 6th April 1955, Nottenbohm Case, Liechtenstein v Guatemala, Judgement 1955 I.C.J., 4 [cited as: Liechtenstein v Guatemala, I.C.J., 4.]
- International Emergency Economic Powers Act, as amended (Public Law 95–223; 50 U.S.C. §§1701–1706; 91 Stat. 1628). Available at <https://www.govinfo.gov/content/pkg/STATUTE-91/pdf/STATUTE-91-Pg1625.pdf>
- Jakhu R, Wilson J (2000) The new United States export control regime: its impact on the Communications Satellite Industry. In: XXV annals of air and space law, 2000, pp 157–181
- Joyner D (2004) Restructuring the multilateral export control regime system. In: Journal of conflict and security law, Oxford University Press, Oxford, United Kingdom, 9(2):181–211
- Konyukhov SN (2003) Conversion of Missiles into Space Launch Vehicles. In: Mark H (ed) Encyclopaedia of space science & technology, vol 1. 441 ff
- Landry KL (2010) Exploring the effects of international traffic in arms regulations restrictions on innovations in the U.S. Space Industrial Base. Air Force Institute of Technology, Wright-Patterson Air Force Base, Ohio, p 63. <http://www.dtic.mil/cgi-bin/GetTRDoc?AD%ADA535245>
- Little KC, Reifman SD, Dietrick AJ (2015) U.S. export controls apply extraterritorially – circumstances in which foreign persons are subject to U.S. export laws and regulations. <http://www.cailaw.org/media/files/SWIICL/ConferenceMaterial/2015/bootcamp/ear-ita-article1.pdf>
- Long C (2013) An imperfect balance: ITAR exemptions, national security, and U.S. competitiveness. 2 Natl Secur Law J 43:58. Arlington (US)
- Marboe I (2012) Soft law in outer space, the function of non-binding norms in international space law. Böhlau, Vienna
- Markoff MG (1976) Disarmament and “Peaceful Purposes” Provision in the 1967 Outer Space Treaty: In Journal of Space Law. University of Mississippi School of Law, Vol. 4, p 6
- Markoff MG (2005) Disarmament and “Peaceful Purposes” provisions in the 1967 outer space treaty. J Space Law 1967:3. Institute of Air and Space Law, McGill University, “Peaceful” and Military Uses of Outer Space: Law and Policy, Feb 2005. Available at [http://www.e-parl.net/pages/space\\_hearing\\_images/BackgroundPaper%20McGill%20Outer%20Space%20Uses.pdf](http://www.e-parl.net/pages/space_hearing_images/BackgroundPaper%20McGill%20Outer%20Space%20Uses.pdf)
- McGraw-Hill Science & Technology Dictionary, accessible at <http://www.answers.com/library/Sci%252DTech+Encyclopedia-cid-3566557>
- Mineiro MC (2012) Space technology export controls and international cooperation in outer space. Springer, Dordrecht/Heidelberg/London/New York
- MTCR, Equipment, software and technology annex 2014, para 1(a);, Category I 1.A.1; Category I 1. B.1. Available online at [http://mtrc.info/wordpress/wp-content/uploads/2016/10/MTCR-TEM-Technical\\_Annex\\_2016-10-20.pdf](http://mtrc.info/wordpress/wp-content/uploads/2016/10/MTCR-TEM-Technical_Annex_2016-10-20.pdf). Accessed 30 Apr 2019
- NASA Advisory Council Regulatory and Policy Committee Observations, Findings, and Recommendations of 12 October 2018. [https://www.nasa.gov/sites/default/files/atoms/files/regulatory\\_policy\\_committee\\_report\\_dec2018\\_tagged.pdf](https://www.nasa.gov/sites/default/files/atoms/files/regulatory_policy_committee_report_dec2018_tagged.pdf)
- Office of Space Commerce (2018) ITAR clarification on satellite thrusters. <https://www.space.commerce.gov/itar-clarification-on-satellite-thrusters/>
- Office of Space Commerce (2019) Space Council focuses on regulatory reform. <https://www.space.commerce.gov/space-council-focuses-on-regulatory-reform/>
- OJL 134 (2009) p 264. Available at [http://trade.ec.europa.eu/doclib/docs/2009/june/tradoc\\_143390.pdf](http://trade.ec.europa.eu/doclib/docs/2009/june/tradoc_143390.pdf)
- Opinion of the Court of 11 November 1975 given pursuant to Article 228 of the EEC Treaty. – Avis 1/75
- Part 121 of the International Traffic in Arms Regulations (ITAR). Available at [http://pmdrtc.state.gov/regulations\\_laws/documents/official\\_itar/ITAR\\_Part\\_121.pdf](http://pmdrtc.state.gov/regulations_laws/documents/official_itar/ITAR_Part_121.pdf)
- Part 734.4 of the EAR. <http://www.bis.doc.gov/policiesandregulations/ear/734.pdf>
- Part 736.2 of the EAR. <http://www.bis.doc.gov/policiesandregulations/ear/736.pdf>
- Part 740.2(a) 7 of the EAR
- Part 764.3 of the EAR. Available at <http://www.bis.doc.gov/policiesandregulations/ear/764.pdf>
- Part 772 EAR. Available at <http://www.bis.doc.gov/policiesandregulations/ear/772.pdf>

- Pezzullo M (2014) Sovereignty in an age of global interdependency: the role of borders. Australian Strategic Policy Institute. Canberra, Australia
- Public Law 105–261 – 17 Oct 1998. Available at [http://www.opbw.org/nat\\_imp/leg\\_reg/US/nat\\_def\\_auth\\_act.pdf](http://www.opbw.org/nat_imp/leg_reg/US/nat_def_auth_act.pdf)
- Regulation (EU) No. 388/2012 of the European Parliament and of the Council of 19 Apr 2012 amending Council Regulation (EC) No. 428/2009 setting up a community regime for the control of exports, transfer brokering, and transit of dual-use items; OJ L 129, 16 May 2012. Available at <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:129:0012:0280:EN:PDF>
- Ress H-K (2000) Das Handelsembargo, völker-, europa- und außenwirtschaftsrechtliche Rahmenbedingungen. Praxis und Entschädigung. Springer, Berlin
- Rhodes Ch, Hough D, Ward M (eds) (2015) The aerospace industry: statistics and policy. Available at <https://researchbriefings.parliament.uk/ResearchBriefing/Summary/SN00928>
- Satellite Industry Association (SIA) – represented by the Tauri Group. 2018 State of the Satellite Industry. Available online at: <https://www.sia.org/wp-content/uploads/2018/06/2018-SSIR-2-Pager.pdf>. Accessed 07 February 2019
- Schrogl K-U, Neumann J (2010) Article IV. In: Hobe S, Schmidt-T B, Schrogl K.-U (eds) Cologne Commentary on Space Law, vol 1, Outer Space Treaty, Carl Heymanns Verlag, Köln
- The Australia Group. <http://www.austaliagroup.net/>
- The current version is Available at [http://pmdtc.state.gov/regulations\\_laws/itar\\_official.html](http://pmdtc.state.gov/regulations_laws/itar_official.html)
- The Export Administration Act of 1979. Public Law 96–72; Enacted September 29, 1979. <https://legcounsel.house.gov/Comps/The%20Export%20Administration%20Act%20of%201979.pdf>
- The Hague Code of Conduct against ballistic missile proliferation, adopted 25 Nov 2002
- The Hague Code of Conduct against ballistic missile proliferation, List of Subscribing States (2019). Available at [https://www.hcoc.at/?tab=subscribing\\_states&page=subscribing\\_states](https://www.hcoc.at/?tab=subscribing_states&page=subscribing_states)
- The International Traffic in Arms Regulations (ITAR), §§ 123 and 125, respectively. Available at [http://www.pmdtc.state.gov/regulations\\_laws/itar\\_consolidated.html](http://www.pmdtc.state.gov/regulations_laws/itar_consolidated.html)
- The International Traffic in Arms Regulations (ITAR), §§ 124.1
- The MTCR Guidelines. Available online at <http://www.mtc.info>. Accessed 20 Aug 2012
- The Nuclear Supplier Group. <http://www.nuclearsuppliersgroup.org>
- The report is available at. [http://www.defense.gov/home/features/2011/0111\\_nsss/docs/1248\\_Report\\_Space\\_Export\\_Control.pdf](http://www.defense.gov/home/features/2011/0111_nsss/docs/1248_Report_Space_Export_Control.pdf)
- The Wassenaar Arrangement on Export Controls for Conventional Arms and Dual-Use Goods and Technologies, opened for signature on 12 July 1996 and entered into force on 1 Nov 1996, guidelines and procedures. Available online at <https://www.wassenaar.org/app/uploads/2015/06/WA-DOC-17-PUB-001-Public-Docs-Vol-I-Founding-Documents.pdf>. Accessed 30 Apr 2019
- The Wassenaar Arrangement Secretariat, List of dual-use goods and technologies and munitions list – public documents volume II of 06 December 2018, pp 221–222. Available online at <https://www.wassenaar.org/app/uploads/2018/01/WA-DOC-17-PUB-006-Public-Docs-Vol.II-2017-List-of-DU-Goods-and-Technologies-and-Munitions-List.pdf> Accessed 30 April 2019
- The White House. President Donald J. Trump is Reforming and Modernizing American Commercial Space Policy (2018). Available online at: <https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-reforming-modernizing-american-commercial-space-policy/>. Accessed 10 Feb 2019
- Tietje C (2009) In: Herdegen M (ed) Internationales Wirtschaftsrecht. Ein Studienbuch. Beck, Munich, p 681
- Treaty Banning Nuclear Weapon Tests in the atmosphere, in outer space, and underwater, signed 5 Aug 1963 and entered into force on 10 Oct 1963. Available online at [http://www.un.org/disarmament/WMD/Nuclear/pdf/Partial\\_Ban\\_Treaty.pdf](http://www.un.org/disarmament/WMD/Nuclear/pdf/Partial_Ban_Treaty.pdf). Accessed 20 Aug 2012
- Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and other celestial bodies (signed 27 Jan 1967, entered into force on 10 Oct 1967) 610 UNTS 205
- Treaty on the Non-Proliferation of Nuclear Weapons, signed on 12 June 1968, entered into force on 22 Apr 1970, reproduced in IAEA INFCIRC/140

- U.S. Department of State (2016) A resource on strategic trade management and export controls. <https://www.state.gov/strategictrade/>
- UN Doc. S/Res/1540 (2004) Text available at <http://www.un.org/News/Press/docs/2004/sc8076.doc.htm>
- United Nations Register of Conventional Arms (UNROCA). Established on 1 Jan 1992 under General Assembly Resolution 46/36 L of 9 Dec 1991
- van Fenema PH (1999) The international trade in launch services: the effects of U.S. laws, policies and practices on its development, Leiden
- von der Dunk FG (2011) National space legislation in Europe, issues of authorisation of private space activities in the light of developments in European space cooperation. Brill, Leiden
- von der Dunk FG, Tronchetti F (eds) (2017) Handbook of Space Law. Edward Elgar Publishing, Cheteham/Northampton
- Wassenaar Arrangement, Initial elements: statement of purposes, paragraph 1
- Wegner C, Weith N, Ehrlich W (eds) (2006) Grundzüge der Exportkontrolle. Bundesanzeiger Verlag, Cologne, Germany
- Wetter A (2009) Enforcing European Union law on exports of dual-use goods. Oxford University Press, Oxford





# Space Systems and Space Sovereignty as a Security Issue

# 12

Annamaria Nassisi and Isabella Patatti

## Contents

Introduction .....	212
Notion of Sovereignty and Jurisdiction .....	212
Why Does Space Security Matter? .....	214
Space Systems and Security from Space .....	215
State Sovereignty and Homeland Security .....	215
State Sovereignty and the Military Domain of a state .....	218
Space Systems and Security in Space .....	220
Vertical Territorial Sovereignty .....	221
Space Systems and Economic Sovereignty .....	223
Conclusion .....	224
References .....	225

## Abstract

Since the beginning of space activities, the global community speculated about the relation between planet Earth and the space environment, and on the potential offered by the space enabled services to safeguard a country's political, economic, and social sovereignty. Through the decades, space technologies progressively enhanced global safety, by improving domestic and international coordination and strategies. In particular, this chapter will focus on the relation between space systems and the security issues linked to a state's sovereignty.

A. Nassisi (✉) · I. Patatti

Strategic Marketing, Thales Alenia Space, Rome, Italy

e-mail: [Annamaria.Nassisi@thalesalieniaspace.com](mailto:Annamaria.Nassisi@thalesalieniaspace.com); [Isabella.Patatti@external.thalesalieniaspace.com](mailto:Isabella.Patatti@external.thalesalieniaspace.com)

---

## Introduction

Space has always been the stage of humankind's greater achievements and the focus of inspiring collaboration among nations, mainly within the scientific domain. The space sector has always been considered a strategic resource, able to contribute to the pursuit of a multitude of political, social, and economic objectives of a country (Darnis et al. 2016). The ability to access to satellite capabilities and operate them has always been critical to both the major powers on the international geopolitical stage and also the global community as a whole. The space environment has acquired greater importance, not only for the institutional actors but also for non-state actors, scientific and academic institutions, international organizations, and all other players that use space technologies and services in order to improve their activities. Outer space resources embrace all kind of applications, ranging from global communications to farming, from weather forecasting to environmental monitoring and climate change, from navigation to surveillance and disaster management. Being critical to the well-being of all countries and people, it becomes imperative that all humankind can access and enjoy its many benefits. Therefore, given its importance and practical utilization, space has become a particularly challenging conundrum of public policy.

Space is also interlinked to the concept of security, safety, and defense. Within the security and safety context, space infrastructures and services are key elements to the political and strategic dimension. Whether we take into consideration international agreements and policies or situation of crisis and disasters, space-based capabilities appear to be strategic and effective instruments, critical to the well-being as well as safeguarding the sovereignty of states. Furthermore, the increase of dual-use space systems, which are blurring the line between military and civil space-based missions, is linked to public returns of investments in proprietary assets. The progress in technological advancements seems today to be inadequately regulated by the 1967 Outer Space Treaty (OST), and an update should be envisaged. In the last years, the concept of space security is being linked to the idea of having a dedicated space force, but this proposal is still being object of discussion among the spacefaring nations. This chapter will focus on the security and defense concerns of space-enabled capabilities linked to the sovereignty and interests of a state, by examining the issue from different angles, in particular those connected to the security, defense, political, and economic dimensions. The objective of this discussion is dual: we want to highlight the importance of space assets as strategic elements for the security and well-being of the sovereignty of a state.

---

## Notion of Sovereignty and Jurisdiction

The increasing awareness of vulnerabilities has led to a debate about state sovereignty. Given that this term carries some weight, it is worth defining it within the context of this discussion. Sovereignty, once a relatively uncontested concept, lately had become a question of rivalry within the national and international relations

theory (Alshdaifat 2018). In the context of contemporary public international law, we can define sovereignty as the basic international legal status of a state that, within its territorial jurisdiction, is not subject to governmental, executive, judicial, or legislative jurisdiction of a foreign state or to foreign laws other than public international law (Steinberger 2013).

Sovereignty is a legal principle by which each state is entitled to exercise exclusive control and supreme authority within its boundaries. Article 1 of the Montevideo Convention of Rights and Duties of states of 1993 indicates “*the state, as a person of international law, should possess the following qualifications: Permanent population, a defined territory, government, capacity to enter into relations with other states*” (Montevideo Convention 1933). Furthermore, Article 2 of the Charter of the United Nations recognizes that all states are equal and sovereign because they all are politically independent. Sovereignty can therefore be considered the benchmark for the doctrines of responsibility, jurisdiction, and nationality. The concept of jurisdiction refers to the power of the states to affect its nationals, property, and circumstances, and therefore reflects the basic principles of sovereignty, equality of states, and non-interference in national affairs. The competence of states in respect to their territories is generally attributed to their sovereignty and jurisdiction, but a distinction in the two terminologies should be noted: while sovereignty can be intended as the legal personality of a state, jurisdiction refers to the rights, claims, powers, and freedoms of a state and therefore refers to its regulatory authority to make and enforce rules upon people.

The notion of sovereignty applied to outer space has been introduced as an object of discussion, following the launches of the first satellites in 1957, and then further developed, with the creation of the OST. in 1967. Articles I and II of the treaty affirm that all space activities shall be undertaken in the sovereignty-free outer space, including the Moon and other celestial bodies. Furthermore, outer space is recognized to be *res communis*, which according to Roman law is the “*property of all,*” that is outer space is not subject to private ownership. However, the exclusion of sovereignty in outer space laws does not exclude the exercise of certain sovereign rights by states in space (Zhang 2019). Article VI of the Outer Space Treaty, as *lex specialis*, recognizes the concept of jurisdiction to be applicable to a state’s activities in outer space, and asserts that states are responsible for all *governmental* and *nongovernmental* space activities. Article VI does not make a distinction as to whether the activities at issue are the state’s own activities or those of private actors. Given that space activities are undertaken by a state (and/or nongovernmental body) by means of objects and infrastructures, a state’s supervision over the said activities invites concurrent jurisdiction over it: this *quasi-territorial jurisdiction* provides space objects with a nationality and converts them into pieces of quasi-territory of a particular state (Von der Dunk 2011). The concerns encompassing the concept of sovereignty, however, have become more critical in recent decades, as the growing lack of natural resources and the need for national security are major issues of the twenty-first century.

In this perspective, also non-spacefaring countries are going to procure or develop their own space infrastructures in order to be independent and to strengthen their own sovereign jurisdiction. As a consequence, the protection of space infrastructures becomes fundamental to guarantee continuity of the space services. The sovereignty of a state could have implications also in the removal of satellites, or part thereof, when it is classified at the end of its life as a debris. New Active Debris Removal (ADR) technology and investments from the private sector have voiced doubts on how to deal with these activities being the satellite, or part thereof, a sensitive element for a state. Analogous considerations can be done for other types of technologies, such as On-Orbit Services (OOS), where the private sector is investing to supply services. There is no clearly defined legal framework that reconciles the sovereignty needs and the return on investment for the private sector.

---

## Why Does Space Security Matter?

At the dawn of the space program, civilian and military space systems were developed by the Soviet Union and the United States according to their respective competitive strategies. In particular, during the years of the Cold War and the nuclear buildup, the two nations wanted to detect the construction of the nuclear arsenals from afar and find storage and preparation sites for the missiles through the use of observation and early warning satellites, which later became one of the benchmarks of the strategic dialogue that opened in the late 1960s. In order to keep outer space a safe environment and prevent its weaponization, in 1967 the Outer Space Treaty was drafted and signed by 132 countries. The idea behind the treaty was to have a dedicated document clearly indicating that the use of space is a privilege for the whole humanity and, hence, state sovereignty cannot be extended to outer space. However, countries started to progressively understand the strategic value offered by the ownership of space assets, and they started to invest more heavily in space activities for competitive, defensive, political, and economic reasons.

Space applications have quickly become a powerful asset in the new geopolitical strategic arena, as governments have started to integrate and use space systems for various purposes. The new role of space activities as a component of state power has opened up new debates nationally and internationally that could radically change the world scene at a political, economic, and industrial level. Although the threat of the Cold War is now over, countries should still be prepared to address a multitude of security problems that could arise without warning and in unpredictable ways.

We can identify two dimensions of security offered by the space environment:

1. *Security from space* that entails the contribution of space systems in achieving enhanced security on Earth and encompasses Earth observation satellites, early-warning systems, navigation satellites, and electronic intelligence systems to guarantee security for the country and for international cooperation, such as food and water security, study of climate change, management of natural resources and disasters, migration, border control, environmental protection.

2. *Security in space* that is focused on the protection of the assets in the outer space environment against natural and human threats.

Over the past decade, international fora have pursued legal frameworks for responsible conduct in space, but as of today, the international community has not reached a general consensus on new laws or regulatory norms. The first step in developing new legal frameworks must be based on a realistic, and holistic, assessment of risks and threats (Hitchens and Johnson-Freese 2016).

---

## Space Systems and Security from Space

Nowadays, the link between space and sovereignty appears to be stronger than ever, and a lot of non-spacefaring countries are in the process of acquiring these capabilities. Governments (civil and military) act as both facilitator and regulator to support national development in order to guarantee independence and autonomy. In the spacefaring nations, government funding supports the technological advancements of their national industries to maintain competitiveness and to support high-performance programs development. This approach has been followed also by the non-spacefaring countries that are motivated by self-sufficiency to serve national policy interests (sovereignty). Accordingly, they procure Earth Observation (EO) space systems equipped with cybersecurity capabilities in order to fulfill a more immediate dual-use role, or they develop their own national manufacturing capabilities motivated by the growth opportunity of qualified labor, and an increase in local industry's competencies. Within the context of homeland security, space assets contribute to strengthen both external and internal security of states together with other platforms (e.g., ground-, air-, and sea-based ones) (Directorate-General for External Policies of the Union 2014). The demand of satellites for security objectives has increased in the last few years motivated also by the growing number of threats, expeditionary missions in remote environments, as well as an increased number in humanitarian relief missions. These operations, and in particular the civilian and humanitarian ones, are likely to characterize the states' security efforts in the years ahead.

## State Sovereignty and Homeland Security

National governments have intensified their commitment to homeland security, increasing their operational activities in domains such as border control and maritime surveillance missions. When contextualizing the development and management of space capabilities for security and defense of a state's sovereignty, it must be borne in mind that a state constantly features both public and private actors. states worldwide are progressively shaping and implementing an inclusive approach to security, one that takes into account synergies among different technologies and services, and tries to make the best of existing resources and

capabilities. The space sector represents a strategic resource, able to contribute to the pursuit of a multitude of political and socioeconomic objectives. As mentioned before, space is also naturally tied to the constantly evolving concept of security, which is not always tied to the offense-defense dimension. In this framework, space assets, encompassing a wide spectrum of performances, can answer to both civil and military needs, originating from the growing number of global challenges (natural and man-made) as well as non-state actors that are present on the international scene. In the face of these new security challenges, a state requires timely and reliable information, either when it is operating on its own territory or when it is involved in international matters. Besides the daily sovereign affairs within its territory, a state must also keep into consideration its commitments towards the global community, borne to safeguard its own interests or necessary to maintain the stability of the international landscape. The production of information relevant to security in the shape of satellite based information, if coupled with in-situ, aerial, and other source of intelligence, represents a strategic tool able to influence decision-making processes at both national and international level.

At national level, security relies on governments, represented by institutional actors (e.g., space agencies, ministers of defense, minister of interior, and minister of foreign affairs, etc.) and is hence related to national sovereignty: in particular, homeland security is an especially critical element in the overall security of a country, as it does not only protect the state from attacks but also ensures the safety of people by helping government bodies to prepare for and mitigate damage from various security threats (Wu and Wang 2018). Effective homeland security operations rely on information collection, integration, and analysis. Hence, a secure and integrated intelligence network is required. The dual-use tied to space-based data and information is particularly useful in making sure that the sovereignty of a state is protected *internally*, through the creation of a stable environment for its people, and *externally*, through the protection of national sovereignty and interests against foreign interference and violation. Remote sensing intelligence can help government bodies in establishing border security and ensure territorial protection by monitoring national borders and territorial seas.

The satellite infrastructure contributes also to the homeland security department in the fight against attacks perpetrated from non-state actors. Institutions and public structures, which are related to the image of a state or are symbolic of a state's power, can quickly become targets of attacks. For example, the attacks of the 11 September 2001 targeted symbols of American power. The term *non-state actor* is a very broad one and can refer to any entity or force that is not directly controlled, integrated into, or legally part of a sovereign state (Boyce 2013). Non-state actors can range from terrorists to ruthless guerrillas, or even to private and commercial entities. One of the top priorities of a country's homeland security is to protect its people from groups or individuals that, for political, religious, or economic motives, engage in terrorist attacks, criminal acts, or actions that threaten national safety and security. In this context, one of the main problems of the protection of national sovereignty is the

possibility of incurring in asymmetric warfare against non-state players engaged in terrorist attacks.

There are many different definitions of terrorism. Some of these would suggest that an act only counts as terrorism if it directly causes death or injury to innocent people, while other definitions are much broader. For the purposes of this chapter, we will define terrorism as the *unlawful use of violence and intimidation (. . .) in the pursuit of political aims* (Oxford English Dictionary). Terrorist acts will differ based on the behavior and characteristic of the criminal group, and how it would respond to different types of government actions. Groups could attack governments or military targets to gain autonomy from their existing regimes, or could attack civilian moved by political or religious motives. Attacks could target a state's technologies: one example was the use of jamming during Operation Iraqi Freedom, in which insurgents deliberately jammed commercial satellite communications used by the US military. In case of an attack against space systems, terrorist groups would more likely engage in cyberattacks (Coleman and Coleman 2017), or in practices to degrade an orbit, or to disable communication links, or blind surveillance satellites to reduce a state's military advantage. For example, the Liberation Tigers of Tamil Eelam (LTTE) frequently hacked government networks and websites to engage in propaganda and, in 2007, pirated a US satellite to broadcast to other countries.

To enhance national security, the market trend highlights major requests to protect the space assets from cyberattacks. Cybersecurity encompasses aspects related to computing and network that will include the satellite and having an impact on all elements within the network topology and connected computers. As a consequence, this capacity extends to data delivery and cloud systems. The protection of space-based assets enables secure data integrity, data availability, data confidentiality, and resilience. A set of regulations, stemming from spacefaring countries, has been put in place to address the business practices with the aim to preserve national security and to comply with international obligations. These regulations are applicable to both institutional and commercial programs, and could help to prevent future non-state actors to acquire their own capabilities in space, with the intent of using them to launch direct attacks. A 2016 research paper stated that *“cyber threats against space-based systems include. . . well-resourced organized criminal elements seeking financial gain; (and) terrorist groups wishing to promote their causes, even up to the catastrophic level of cascading satellite collisions”* (Livingstone and Lewis 2016). It is important to not underestimate non-state actors that carry out asymmetric attacks to influence states, and this is true for the space segment as it is for the ground one. According to Miller (2019), *“current technology makes space an offense-dominant domain. Despite the cost and technological difficulty of reaching space, it is relatively easy to carry out attacks, at least compared to the cost of defending capabilities in space.”* Therefore, it is important to develop defense capabilities in the space domain in order to reduce the chances of an attack and be prepared in case of one.

## State Sovereignty and the Military Domain of a state

With respect to the relationship between state sovereignty and military space operations, the potential of space capabilities for military operations represent a key element in the analysis of space as a strategic resource of a state. In particular, military reconnaissance came to be viewed as a staple in a state's exercise of territorial sovereignty, whereas having knowledge of the adversary's military and industrial abilities was considered essential to receive an accurate situational awareness and to prevent foreign intervention. Even today, despite the proliferation of scientific and commercial satellite data, the technology's military roots continue to be evident: for example, defense departments still control the lion's share of high-resolution satellite imagery.

The prominence of the defense domain continues to be of critical importance in safeguarding the sovereignty of a state. As it is often remarked, the security of its own citizens, who gave their allegiance to the sovereign entity, is the first duty of a state. Hence, with this consideration in mind, the use of the defense industry to assure the safety of its citizens and security of its territory against internal and external threats can often become a necessary function (Yeo 2014). Overarching goals, both civilian as well as military, have been defined and adapted to match the changing security environment. Space assets can provide strategic help to support the operative theaters in case of international cooperation for crisis management operations. Significant changes feature not only the miniaturization of technologies for small satellites but also the launch services encompassing new generation low-cost launchers that offer speedy rocket launches in short time

### Military Activity in Space

It is worth mentioning that the legality of military activities in space is tied to the 1967 OST (de Gouyon Matignon 2019). Most significant from a military perspective is Article I, which stipulates that space is “*free for exploration and use by all states without discrimination of any kind, on a basis of equality and in accordance with international law and there shall be free access to all areas of celestial bodies,*” hence not explicitly prohibiting the use of satellites to perform surveillance, reconnaissance, communications, and other functions without authorization of other states, even during peacetime. Other articles of the OST bear on the military use of outer space, such as Article IV, which calls for the de-weaponization of space: “*States Parties to the Treaty undertake not to place in orbit around the Earth any objects carrying nuclear weapons or any other kinds of weapons of mass destruction, install such weapons on celestial bodies, or station such weapons in outer space in any other manner. The Moon and other celestial bodies shall be used by all states Parties to the Treaty exclusively for peaceful purposes. The establishment of military bases, installations and fortifications, the testing of any type of weapons and the conduct of military maneuvers on celestial bodies shall be forbidden. The use of military personnel for scientific research or for any other peaceful purposes shall not be prohibited. The use of any equipment or facility necessary for peaceful*



*exploration of the Moon and other celestial bodies shall also not be prohibited.*” Historically, military space operations have been nonthreatening in character and raised very few contentious legal issues. They have typically consisted of space control (passive defensive counter space missions) and space support, while space warfare has always remained purely notional. The legal architecture governing military operations in space was originally designed for space exploration and commercial applications, and the resilience of the applicable law in the face of the challenges arising from the changes in the global political landscape has yet to be determined (Schmitt 2006).

### **Peaceful Use in the Defense Domain**

There are questions about the interpretation of the term *peaceful* as it can be intended as either *non-military* (broad interpretation) or *non-aggressive* (narrow interpretation). In particular, the narrow interpretation could explain how it is imperative for a nation to retain its right of self-defense, as expressed both in customary law and in Article 51 of the Charter of the United Nations. For example, the United States provide that the term “peaceful purposes” allows for “*intelligence-related activities in pursuit of national defense*”. Through this, it is possible to adopt a “battlefield awareness” model, thanks to which the programs that have defense purposes can focus on information collection for tactical applications. In this sense, space systems are viewed as strategic enablers that offer better knowledge to a state’s military operations through value-added information that increase the ability of a state to apply precision military force. National military bodies can rely on space support provided by numerous kind of satellites, such as Satellite Communications (SatComs), Intelligence, Surveillance and Reconnaissance (ISR), Position Navigation and Timing (PNT), although potential adversaries could develop anti-satellite skills, that, supported by an array of sensors, would be able to attack space systems through multiple manners (e.g., cyber, electronic, missiles, directed energy weapons, jamming) (Defense Intelligence Agency 2019). The level of modernization of technologies has completely reinvented satellite utilization in modern warfare, where battles can be won or lost depending on who has the most sophisticated, secure, and specialized infrastructure. Space offers persistent coverage, and, unlike ground vehicles or aircrafts, satellites are unfettered by earthly features such as atmospheric drag or terrain. Through remote sensing real-time intelligence, military targets can be detected and battlefield features (e.g., ground terrain, weapon equipment, enemy location) can be unveiled and a strategic support within the operative theater can be provided.

Satellites offer capabilities to monitor and, in addition, provide warning messages against the transportation and launch of ballistic missiles and enemy movements inside and outside a country’s frontier. Navigation systems deliver guiding information to accurately strike targets. Space-based sensors provide the first indication of attacks and terrestrial sensors provides follow-up information useful for countries to deliver the appropriate defensive and/or offensive response. The space dimension becomes indispensable to answer to the prerequisites of precision, efficacy, and promptness that are essential to military operations.

## The Dawn of New Regulations and Space Policy Directives

As we have seen, nowadays, space systems represent a significant constituent of national defense by means of aiding government bodies in the creation of an active and dependable defense strategy. In recent years, a number of countries have started to recognize space as a distinct location or concept where conflict can take place, such as on land, sea, air, or space, or within digital systems (Liptak 2019). Indicative of the likelihood of the space domain to become more and more interlinked with the defense industry are, indeed, the 2019 recent events, which saw the re-establishment by the Trump's Administration of the U.S. Space Force, followed closely by the creation of the French Space Command by President Macron. Born as a way of "proactive prevention," the newest branch of the American and French forces will protect the interests of their respective countries in space. In the wake of these events, also the North Atlantic Treaty Organization (NATO) turned its attention to space as an "*operational domain*" over concerns that enemies of the Western military alliance could cause chaos by jamming satellites. NATO's Secretary General Jens Stoltenberg reportedly said that there was no question of weapons being deployed, but the alliance had to protect civilian and military interests (Boffey 2019). There will always be a case of discrepancy between the non-territorial nature of space and the principle of state sovereignty, whereas the notion that the jurisdiction, affairs, and entities within a territory are solely business of that territory becomes more complex when there are no physical lines. However, given the defense department role and use of resources in space for the purpose of national defense, and for the purpose of this discussion, reference should be made to Article VI of the OST that attributes the responsibility of the activities of the governmental entities and their contractors to states.

---

## Space Systems and Security in Space

One of the fundamental principles of the concept of sovereignty of a state is autonomy. In the modern international system, countries continue to perceive themselves as independent units and strive to preserve their autonomy and decision-making ability. The space systems are classified as critical infrastructures on which states rely for their well-being. As technological and cost barriers to space lower, more countries and private entities partake in space infrastructure construction and rely on ownership of space assets.

Today, a significant proportion of the economies and infrastructures of modern states depend on such technologies. In this framework, it is easy to see how space-based service interruption would severely affect a large number of activities. Thus, protecting them by reducing their vulnerability is becoming critical for the sovereignty of a state.

There are several cases of space threats that would put at risk the safety of infrastructures in space, such as space-debris collisions, or the uncontrolled reentry of a spacecraft. Other than uncontrolled disasters, with the rapid increase in space

technologies comes also the risk of utilizing space systems for direct attack purposes (e.g., North Korea recently tested ICBMs missiles to ascertain they can use these weapons against Japan and the United states). Space debris around the Earth constitute a considerable hazard to both crewed and unmanned space operations. Objects in LEO could impact or be impacted by pieces of debris, and the force generated by the impact could be so powerful to damage or render inoperable the satellite or even create more debris, causing a collisional cascade effect known as Kessler Syndrome.

Another threat to space assets could be represented by adversaries jamming communication and navigation systems, or blinding imagery satellites or other strategic sensors. Physical or cyberattacks against ground infrastructures can also threaten space assets capabilities. The outer space and cybernetic environments have been intertwined. Hence, they find themselves facing common threats that they would need to be addressed by common strategies. In particular, it is worth reminding the attack against NASA in 2010–2011, in which NASA's computers experienced more than 5,400 incidents of unauthorized access and attacks by malicious software (Protalinski 2012). According to the investigations carried out, the attacks may have come from individuals wanting to test their abilities, foreign intelligence services and criminal enterprises wanting to profit from the information gained.

The international community needs to recognize the level of dependence modern societies have on space assets and capabilities. Many institutional and private actors rely on the space sector to create a set of strategies, initiatives, and programs at a national and international level. The last few years have seen a rekindle of the strategic great-power competition for the conquest of the space environment, which has become object of interest of the major global actors. China and the United states, as in other dimensional domains, are first in line in the newest space race, especially when it comes to strengthening their position in an environment that has numerous implications, particularly economic and strategic. Compared to the historical space race of the United states versus the Soviet Union, the newest race sees the involvement of numerous countries, other than the aforementioned China and the United states: even though Russia remains a great power in the space segment, other countries like France, Israel, India, and Japan are making their voices heard. As the new space race reaches the heart of the competition, it could have a strong impact on the balance of power in the world. How this will affect to the concept of state sovereignty remains to be seen and should be the object of investigation by policy makers.

## **Vertical Territorial Sovereignty**

The debate over the delineation of the boundary between outer space and state sovereignty precedes the beginning of the space race; however, following the launch of Sputnik in 1957, two legal concepts concerning spaceflight started to be the object of discussion of policy makers. Originally, when the United states and

the Soviet Union started their expansion towards outer space, they tacitly assumed that international law did not prohibit it, and the other countries did not protest as well. Today, following the ever-changing space technology, it is easy to notice how the understanding and implementation of a state's sovereignty in outer space needs to be addressed legally. A state's sovereignty remains important for the security of the state. As of today, the delimitation of outer space and airspace is still not regulated and therefore sovereignty cannot be presumed. It has happened that disagreements arose in this matter, like in the case of the 1976 Bogotá declarations regarding the supremacy of equatorial states over geostationary orbit (Polkowska 2018).

Concerning vertical extension of sovereignty, it should be recalled that according to the Chicago Convention of 1944, states hold absolute and exclusive jurisdiction in relation to their respective air space. However, the 1967 OST establishes that outer space cannot be subjected to national claims of appropriation (Bittencourt Neto 2012). The problem of defining a state's extension of vertical sovereignty is primarily based on the lack of a natural boundary separating air and space. In the years following the Chicago Convention, states have taken different positions on the matter, but as of today, there is still no general consensus. For example, after the launch of the Sputnik, the Soviet Union claimed vertical sovereignty without a defined upper limit. South Africa, on the other hand, pinned down outer space as *"the space above the surface of the Earth from a height at which it is in practice possible to operate an object in an orbit around the Earth."* The United States' position in the matter changed repeatedly between the 1950s and 1960s, yet with a 2003 regulation, and with the purpose of defining the qualifications of an astronaut, the U.S. Air Force defined *space* as the area of 50 miles (80.4 km) above the Earth's surface (Reinhardt 2007). The attitude of states generally varies depending on the current political and economic situation. However, the exercise by the state of unlimited control and power in the air is also a condition for the security of the state and its citizens (Shrewsbury 2003). The security issue is therefore an essential argument in favor of the concept of territorial authority.

Delimitation is also important to ensure equal access to space for all states. In the words of John Cobb Cooper, *"unless [the upper boundary of national airspace] is fairly close to the Earth's surface, few states will be able to put a satellite into orbit... without passing through the national airspace of other states. In other words, few states will be free of a political veto by other states in planning orbital flights."* As more and more states are developing their own domestic space launch capability, only few of these new space powers will be able to freely access space, or utilize the most efficient launch azimuths, if neighboring states can claim sovereignty up to even 62 miles (100 km). Setting a low vertical limit on state sovereignty will ensure all states have equal access to space (Reinhardt 2007).

Another issue raised by the absence of an international definition of the space boundary is liability for space activities. The *Liability Convention* imposes absolute liability on the launching state for damage caused on the surface of the Earth or to aircraft in flight by the state's *"space object"* or the *"launch vehicle and parts thereof,"* as in the case of the uncontrolled reentry of the Soviet Union satellite Kosmos 954 over northern Canada.

As space becomes more and more economically and politically important due to the inexorable progress of science, the issue of vertical sovereignty will continue to grow. Defining the limit between a state's sovereign territory and free outer space could also add clarity to all the treaties that are written in a functional manner without defining where space begins.

---

## Space Systems and Economic Sovereignty

In a world of mutual dependence, economic sovereignty hinges on the ability to protect economic power. In order to safeguard its sovereignty, the aim of a state should be to become a player in all fields that are vital for the resilience of the economic system, and that could contribute to shape the global community's future in a critical way. Today, economic sovereignty becomes a geopolitical power and economic relationships can be used as broader geostrategic goals.

The economic sovereignty agenda of a country should hold several objectives, such as boosting a state's research, scientific and technological base, protecting assets critical to national security, promoting a level playing field in national and international competition, and employing policies to strengthen a state's monetary and financial autonomy (Leonard et al. 2019). The concept of economic sovereignty inspired major initiatives in fields such as energy, geopositioning, artificial intelligence, computing and, of course, aerospace. Space is considered by states a strategic economic domain as it is a major enabler and multiplier (Zervos 2017), while being borderless and virtually unregulated by existing treaties. This characteristic makes outer space one of the main tactical elements of a country and offers states numerous opportunities for leadership and partnerships.

In the consideration of space applications within the economic dimension, it is important to remember that space applications are considered *public goods*, and hence, since the dawn of the space race, they have been mainly funded by public investments. The underlying rationale for public space investments is the concept of *market failure*. Space is an *externality-inducing* industry, and thus governments are needed to manage the externalities into a socially optimum outcome. Furthermore, there is a risk linked to the *underinvestment* within the upstream segment of the space value chain and the long development of programs, commonly regarded as high-risk (Return from Public Space Investments 2015). As a result of these market failures, together with the security considerations associated with the space technologies, the responsibility for production and control of space assets has been historically laid on government institutions. The latter in turn reap the benefits in the form of direct revenues, of territory and disaster management, and indirect revenues, in the form of education and qualified employment. Space activities stimulate the development of new technologies – as an innovation factor, as a competitiveness factor, and as a key to the consolidation of national industrial capabilities and internationally recognized economic power on the world stage. In a world where international alliances are of particular importance for national and worldwide security, the inter-alliance specialization offered by space becomes critical for stability and economic profile of states. A state's strategic autonomy is strengthened by national ownership of

assets for the defense and security applications. It is worth mentioning also that the space industry is subject to economies of scale and scope. In this context, it is possible to notice that space technologies can boost the economic growth of a nation and establish the technological advantage of countries. This is illustrated in the case of the military satellites, which the spacefaring nations domestically produce, due to both the demand side of the country (countries tend to select their home industries to enhance their economies of scale and scope, other than for security reasons) and also the supply side (on which trading restrictions are applied in order to safeguard technologies as trade can rapidly diminish technological gaps).

In particular, the export restrictions play a significant role within the sovereignty of a state (Noble 2008). Keeping the technological edge is perceived as a form of dominant power from countries. As the demand for space-based security is very high, when it comes to exporting major space powers are inclined to protect critical technology. As national security issues are gaining prominence everywhere, so is the relationship between national security and economics. As economics is becoming again an area of great-power competition, economic tools are employed to secure geopolitical advantage. The strategic intent of export control is to keep sensitive technologies out of the hands of potential adversaries and guarantee to a particular state a larger market share. Export control of space technologies in a particular state are, usually, more concerned with the relative performance of foreign systems to those of the state of origin. It is important to protect a country's technological lead and strategic independence through the prevention of the proliferation of technologies and systems to potential adversaries. This is compatible with space systems, as well as the strategic nature of space security, and the fact that industries subject to economies of scale have been long considered strategic to the sovereignty of a country.

However, it is important to keep in mind that economic sovereignty does not mean containing the spread of technology at all costs. In the current interconnected world, technological leadership also depends on continuous innovation and investments benefits stemming from cooperation. While it is important for a state's sovereignty to protect its core assets – especially when security interests are at stake – economic sovereignty does not mean resisting to globalization. A state's competitive advantage also helps to increase the qualified human capital at a remarkable rate. In every business environment – and undoubtedly in the space sector – it is vital to have access to individuals with technical training. An educated workforce fuels the economy of innovation of a state. Accordingly, innovation creates competition and competition creates jobs that, in turn, create growth. Space activities also impact the economic sovereignty of a state through their ability to increase dramatically the capacity of humans to act and to interact with other people or countries with increasing strength (European Space Agency 2005).

---

## Conclusion

Through this discussion, we have seen what important effects space has on modern sovereignty. Space systems reinforce the exclusive structure of sovereignty and its potentiality to foster decisions within its territory and on the world stage. To prosper

and preserve their independence in a world of geopolitical competition, states must address globally the space and security challenges. This could involve creating a new idea of sovereignty that sees the space environment as part of their identity, power, and bureaucratic interests. Creating an environment tailored to such incentives requires work to be done at the legal and policy levels.

---

## References

- Alshdaifat SA (2018) Who owns what in outer space? Dilemmas regarding the Common Heritage of Mankind. *Pécs J Int Euro Law* 2018/II:24
- Bittencourt Neto O (2012) The elusive frontier: revisiting the delimitation of outer space. IAC-12. E7.1.9. <https://iislweb.org/docs/Diederiks2012.pdf>
- Boffey D (2019) Nato leader identifies space as the next 'operational domain', *The Guardian*. <https://www.theguardian.com/world/2019/nov/20/nato-identifies-space-as-next-operational-domain>
- Boyce J (2013) Surrendering sovereignty: the private military industry, the state, and the ideology of outsourcing. [https://skemman.is/bitstream/1946/14746/2/snidmat\\_ma\\_i\\_stjornmalafrædi\\_0.pdf](https://skemman.is/bitstream/1946/14746/2/snidmat_ma_i_stjornmalafrædi_0.pdf)
- Coleman N, Coleman S (2017) Terrorism in space. Examining the issues and mitigating the risks. In: 68th International Astronautical Congress (IAC), Adelaide, Australia, 25–29 Sept 2017
- Darnis J, Sartori N, Scalia A (2016) Il futuro delle capacità satellitari ai fini della sicurezza in Europa: quale ruolo per l'Italia? IAI, Edizioni Nuova Cultura, Quaderni
- De Gouyon Matignon L (2019) The legality of military activities in outer space. <https://www.spacelegalissues.com/space-law-the-legality-of-military-activities-in-outer-space/>
- Defense Intelligence Agency (2019) Challenges to security in space. Defense Intelligence Agency, Washington, DC. [https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space\\_Threat\\_V14\\_020119\\_sm.pdf](https://www.dia.mil/Portals/27/Documents/News/Military%20Power%20Publications/Space_Threat_V14_020119_sm.pdf)
- Directorate-General for External Policies of the Union (2014) Space, sovereignty and European security: building European capabilities in an advanced institutional framework. Publications Office, Luxembourg. [http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/433750/EXPO-SEDE\\_ET\(2014\)433750\\_EN.pdf](http://www.europarl.europa.eu/RegData/etudes/etudes/join/2014/433750/EXPO-SEDE_ET(2014)433750_EN.pdf)
- European Space Agency (2005) The impact of space activities upon society. ESA, Noordwijk. <http://www.esa.int/esapub/br/br237/br237.pdf>
- Hitchens T, Johnson-Freese J (2016) Toward a new national security space strategy. Atlantic Council Strategy paper no. 5. [https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/AC\\_StrategyPapers\\_No5\\_Space\\_WEB1.pdf](https://espas.secure.europarl.europa.eu/orbis/sites/default/files/generated/document/en/AC_StrategyPapers_No5_Space_WEB1.pdf)
- Leonard M, Pisani-Ferry J, Ribakova E, Shapiro J, Wolff G (2019) Redefining Europe's economic sovereignty. European Council on Foreign Relations, Policy Contribution 31321 Issue n°9, Bruegel. [https://www.bruegel.org/wp-content/uploads/2019/06/PC-09\\_2019\\_final-1.pdf](https://www.bruegel.org/wp-content/uploads/2019/06/PC-09_2019_final-1.pdf)
- Liptak A (2019) France's air force is getting a space command. <https://www.theverge.com/2019/7/13/20693087/france-military-air-force-space-command-president-emmanuel-macron>
- Livingstone D, Lewis P (2016) Space, the final frontier for cybersecurity? Research paper, Chatham House International Security Department, London
- Miller GD (2019) Space pirates, geosynchronous guerrillas, and nonterrestrial terrorists. *Air Space Power J* 33:33
- Montevideo Convention on the Rights and Duties of states, Art. 1, 1933, 165 LNTS 19
- Noble MJ (2008) Export controls and United states space power. *Astropolitics* 6(3):251–312. <https://www.tandfonline.com/doi/full/10.1080/14777620802469798>
- Polkowska M (2018) Limitations in the airspace sovereignty of states in connection with space activity. <https://pdfs.semanticscholar.org/cbbb/ebd8da928ea965653bbd6708b8bbfc0cfa0.pdf>
- Protalinski E (2012) NASA: hackers had "full functional control, ZDNet. <https://www.zdnet.com/article/nasa-hackers-had-full-functional-control/>
- Reinhardt DN (2007) The vertical limit of state sovereignty. *J Air Law Com* 72:65. <https://scholar.smu.edu/jalc/vol72/iss1/4>

- Return from Public Space Investments – an initial analysis of evidence on the returns from public space investments. (2015). London Economics IV. <https://londoneconomics.co.uk/wp-content/uploads/2015/11/LE-UKSA-Return-from-Public-Space-Investments-FINAL-PUBLIC.pdf>
- Schmitt MN (2006) International law and military operations in space, Max Planck Yearbook of United Nations Law Online 10:89–125. [https://www.mpil.de/files/pdf3/04\\_schmittii1.pdf](https://www.mpil.de/files/pdf3/04_schmittii1.pdf)
- Shrewsbury MSM (2003) September 11th and the Single European Sky: developing concepts of airspace sovereignty. *J Air Law Com* 68:115
- Steinberger H (2013) Max Planck Institute for comparative public law and international law. In: *Encyclopedia for public international law*, vol. 414. Oxford University Press, Oxford
- Von der Dunk FG (2011) The origins of authorisation: article VI of the outer space treaty and international space law and international space law. *Space, Cyber, and Telecommunications Law Program Faculty Publications*. 69. <https://digitalcommons.unl.edu/cgi/viewcontent.cgi?article=1068&context=spacelaw>
- Wu X, Wang J (2018) *Space system as critical infrastructure*. Springer, Boston
- Yeo AI (2014) Security, sovereignty, and justice in U.S. overseas military presence. *Int J Peace Stud* 19(2):43–67
- Zervos V (2017) The European space-industrial complex: new myths, old realities. *Econ Peace and Sec J EPS Pub* 12(1):28–36
- Zhang W (2019) Extraterritorial jurisdiction on celestial bodies. *Space Policy* 47:148–157





Alexandru Georgescu

## Contents

Introduction .....	228
Critical Infrastructure Protection .....	228
Critical Space Infrastructures .....	231
Distinguishing Characteristics of SI and CSI .....	233
Critical Space Infrastructure Protection .....	234
Results from Framework Application .....	236
Principles of Resilience .....	237
Complex System Governance .....	240
Conclusions .....	242
References .....	242

## Abstract

Space systems are a key enabler for a wide variety of applications which have become critical to the functioning of modern societies. This chapter uses the Critical Infrastructure Protection framework to argue that space systems may constitute a new form of critical infrastructure, dubbed Critical Space Infrastructure, and traces the positive impact that such a perspective may have on space security governance. Critical Infrastructure Protection has developed a conceptual toolbox, as well as practical policy prescriptions, which may be of use to policy and decision-makers to increase resilience and meet future space security challenges.

## Keywords

Critical infrastructure · Resilience · Space systems · Governance · Complex system

A. Georgescu (✉)

National Institute for Research and Development in Informatics (ICI), Bucharest, Romania

e-mail: [alexandru.georgescu@ici.ro](mailto:alexandru.georgescu@ici.ro)

## Introduction

Space systems have become a key enabler for a wide variety of applications related to command, control, coordination, data gathering, and communications. With their growing capabilities and numbers, the quantity and quality of applications also increase, while lowering access barriers, thereby improving usability and leading to an increase in the number of beneficiaries.

The Organisation for Economic Co-operation and Development (OECD) (2016) notes that the world is entering a fifth stage of space development, one in which we are witnesses to “growing uses of satellite infrastructure outputs (signals, data) in mass-market products and possibly for global monitoring of treaties (land, ocean, climate), third generation of space stations, extensive mapping of solar system and beyond thanks to new telescopes and robotic missions, new space activities coming of age (e.g. new human-rated space launchers, in-orbit servicing).” Space inputs permeate many of the products (tangible and intangible) that we consume, which are the result of extensive global supply and production chains or of the processing of information and the combining of symbols within globalized networks.

Therefore, space services may be consumed directly or indirectly through their role in the functioning of other systems on which we are dependent. The use of space capabilities in energy, transport, financial markets, agriculture, weather forecasting, and other fields is well-known. These latter systems represent a small cross-section of critical infrastructures (CI), sociotechnical systems whose disruption or destruction would generate significant economic damage, casualties, and loss of confidence (Gheorghe et al. 2018, p. 3). Their security is paramount and, therefore, we must consider the question of their governance. While government deals with decision-making, governance encompasses mechanisms, norms, and organizations that mediate the decision-making and implementation process.

The governance of the aforementioned infrastructures like energy and transport relies on Critical Infrastructure Protection (CIP), a comprehensive framework for managing the risk to the key infrastructures, assets, and resources on which our societies are critically dependent, which has been developed for the past two decades.

This chapter aims to introduce space systems into the CIP framework and define them as Critical Space Infrastructures (CSI), arguing that CIP can close some of the gaps that have manifested in the governance of space security and which are creating significant troubles from the perspective of sustainable exploitation of space. With the articulation of the existence of CSI, we follow up with a discussion on Critical Space Infrastructure Protection (CSIP) from the perspective of the specialty literature.

---

## Critical Infrastructure Protection

CIP was first conceived during the Clinton Administration, but only came to the fore after the September 11 attacks, when the systemic impact of the attacks was noted and provided ample argument in favor of the defining trait of CIP, the

interdependencies between components, infrastructures, and systems which lead to the transmission of risk and the cascading disruption of critical infrastructures. Presidential Decision Directive (PDD)-63 (1998) identified critical infrastructures as being “those physical and cyber-based systems essential to the minimum operations of the economy and government” (The White House 1998). CIP did not stay confined at the national level. Later, the EU would create its European Program for Critical Infrastructure Protection (EPCIP) through which it set guidelines for improvement of national CIP governance and the identification, designation, and protection of European Critical Infrastructures. Directive 114/2008 established that European Critical Infrastructures are “essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people” and are distinguished from national CI through their impact on two or more Member States “as a result of the failure to maintain those functions” (European Commission 2008).

CIP works most often with the concept of resilience, which is the capacity or quality of a system to retain or rapidly regain an adequate level of functioning in the face of a crisis event, with minimal disruption, material damage, or loss of human life. Linkov et al. (2014) argued that resilience should be a priority from the design phase of new systems and of their regulatory frameworks, because resilience is the only consistent answer to the issues of uncertainty and complexity. CIP also works with numerous other concepts, which encompass different aspects of CI qualities, behavior, and interactions during crisis events (Table 1).

Interdependencies are a key feature of CIP systemic thought. Gheorghe and Schläpfer (2006) define interdependencies as bidirectional relationships wherein the status of one infrastructure affects the status of others and is affected in its turn by others. The topology of critical infrastructure risk is built also with the mapping of interdependencies. These are varied, being physical, sectoral, geographic, logical, social/political, cybernetic, or informational and with many taxonomies in existence. The other key features are the dynamics of cascading disruptions – “cascading disasters are extreme events in which cascading effects increase in progression over time and generate unexpected secondary events of strong impacts. These tend to be at least as serious as the original event and contribute significantly to the overall duration of the disaster’s effect” (Pescaroli and Alexander 2016). They result from the vulnerabilities and rigidities that accumulate within a system-of-systems across multiple domains until a trigger event or mechanism manifests alongside the alignment of key breaking points. The absence of these alignments prevents the actual cascading disruption event, as it interrupts the vector for the transmission and escalation of the disruption. Pescaroli and Alexander (2016) distinguish between cascading effects and cascading disasters. The former are the multidimensional and complex dynamics which produce the latter.

Regionalization and globalization have brought these issues to the fore, as cooperation becomes a key facet of CIP efforts when global supply and production chains as well as globally synchronized databases and markets produce new risks, vulnerabilities, and threats which are beyond the ability of single jurisdiction authorities to tackle. If chains are only as strong as their weakest links, decision-makers and CIP practitioners cannot count on localized resilience and CIP success to

**Table 1** An overview of concepts related to resilience. (Source: author compilation)

Concepts related to resilience in CIP specialty literature	
Vugrin et al. (2011)	
Absorptive capacity	An internal quality of the system that allows it to absorb the effects of systemic or environmental disruption with little degradation in functioning. It is associated with robustness and the presence of redundancies
Restorative capacity	The system recovers easily from the effects of a disruption and also experiences permanent modifications as a result of the episode (adoption of new technology, reorganization, etc.)
Adaptive capacity	The system reorganizes itself in order to maintain functionality, reduce disruptive impact, and rapidly recover full function levels. For instance, a factory may switch suppliers or modify its designs to limit the impact of resource scarcity
Jonkeren et al. (2012)	
Static resilience	The ability of a system to continue functioning after suffering a major shock
Dynamic resilience	The rapidity with which a system recovers from a disruptive event. It is related to repair and reconstruction times
Rockefeller and Arup (2014)	
Reflectivity	Such a system is conscious of the uncertainties and of the changes in the security environment
Robustness	The system actively eschews designs which render it vulnerable to cascading disruptions, catastrophic malfunctions, and overdependence on certain assets
Redundancy	Is found in the diversity of pathways and options for fulfilling system tasks. A system with redundancies can weather significant increases in pressure, upstream shocks, or the malfunctioning of individual assets and system components
Flexibility	The quality that a system possesses to change as a result of shocks and to even find benefits in those changes
Adaptability	The capacity to mobilize systems and resources during temporary stresses or shocks in order to attenuate the impact of the negative events
Inclusivity	The system seeks out and accepts inputs from all categories of stakeholders and includes it in the process of developing strategies, plans, priorities, and resource distribution patterns
Integration	An integrated system responds efficiently to challenges and features short and rapid feedback channels. The governance mechanisms transcend sectorial and other limitations in order to adequately reflect the complexity of the system and to adequately implement policies and decisions

maintain systemic integrity. Helbing (2013) emphasized that global critical infrastructure networks facilitate the propagation of risks and generate the potential for cascading disruption stemming not just from external factors (such as attacks, sabotage, natural disaster) but also from internal ones resulting from system errors, attrition, malinvestment, lack of maintenance, and, most important of all, the complexity of the system-of-systems (SoS). These disruptions within the SoS may lead to the contagion and the escalation of the effects, sometimes in a mutually reinforcing pattern. Perrow (1999) discussed the “normal accidents” or spontaneous malfunctions that arise from the complexity and tight couplings of a system, sometimes without the possibility having ever been foreseen. Eusgeld et al. (2011)

argue that a SoS perspective acknowledges that the components of infrastructure systems may be large-scale systems as well, sometimes operating autonomously from a legal, administrative, or governance standpoint, but linked to the wider system through dependencies and interactions which assign systemic consequences to localized disruptions through the propagation of risks and disruptions.

There was a tacit acceptance of these risks, to the extent to which they were anticipated, in exchange for the efficiencies and gain in well-being that accompanied them. If one were to describe the evolution of CI in the past hundred years, it is that formerly autonomous and vertically integrated infrastructure systems separated by geography, information lag, and risk aversion suddenly found themselves in much greater contact (Bucoveţchi et al. 2019), a situation which Setola et al. (2017) called “rapid change in the organizational, operational and technical aspects of infrastructures.” Cyber infrastructures and now space infrastructures are some of the initiators and facilitators of systemic changes which result in the increase in CI SoS surface contact and in the tightening of the couplings within the system that accelerate the transmission of risk. The systemic transformations give rise to new sources of added value, new functionalities, and also punctual increases in safety and security through higher governance capacity, but also new risks, vulnerabilities, and threats.

The field is constantly evolving to keep pace with the demands of a SoS beset by and in thrall to growing complexity. One of the recent evolutions, for instance, is complex system governance (CSG), which emphasizes complexity as a source of emergent and sometimes unanticipated behaviors and properties in the system not found in its individual components. A later section of the chapter will elaborate on this idea.

---

## Critical Space Infrastructures

OECD (2019) defines space economy as the “the full range of activities and the use of resources that create and provide value and benefits to human beings in the course of exploring, understanding, managing and utilizing space. Hence, it includes all public and private actors involved in developing, providing and using space-related products and services, ranging from research and development, the manufacture and use of space infrastructure (ground stations, launch vehicles and satellites) to space-enabled applications (navigation equipment, satellite phones, meteorological services, etc.) and the scientific knowledge generated by such activities. It follows that the space economy goes well beyond the space sector itself, since it also comprises the increasingly pervasive and continually changing impacts (both quantitative and qualitative) of space-derived products, services and knowledge on economy and society.”

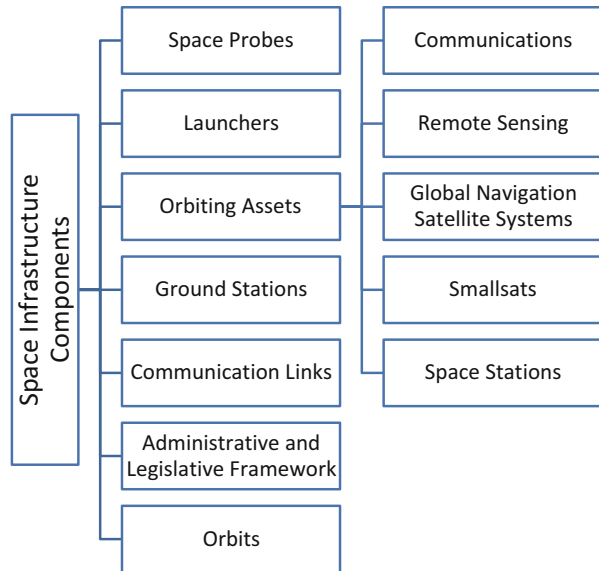
Infrastructure serves not only the economy but also society, and we may draw on this definition to define a space infrastructure (SI) as a sociotechnical system whose main functional component is located beyond the arbitrary line separating the Earth’s atmosphere from outer space. Critical Space Infrastructures have the added trait of criticality – their disruption or destruction would cause significant casualties,

economic damage, or loss of confidence. CSI have components that are also intra-atmospheric – for instance, ground stations and communication links (Fig. 1).

The identification and designation of CI serves an important role in CIP processes, but this tendency may be muted in space. A country may have tens of thousands of miles of roads, serving a large number of settlements of all sizes, which makes the designation of the critical ones for national functioning and continuity in the face of attacks all the more important. However, SI do not have an especially large inventory, given the high number of functions they serve and the number of beneficiaries. For the rest of the chapter, we will discuss CSI primarily as a function of orbiting assets, or satellites. As the field develops, we will one day be able to talk about CSI composed of probes, research bases on other planets, and interplanetary transport networks. As of yet, a theoretical threshold of criticality will likely only be met by SI containing satellite components. The only other likely candidates are the various probes which measure the activity of the Sun and are part of early warning systems regarding solar flares that give CI operators opportunities to enter conservation states or initiate measures to safeguard system integrity. If we were to speculate on the criticality of early warning systems for another high-impact, low-frequency event – the collision of the Earth with asteroids – we would find that operational assets are also located on Earth or in orbit.

According to the frequently updated open-source database of the Union of Concerned Scientists, by 31 March 2019, there were 2062 satellites in orbit (UCS 2019). Table 2 breaks down that number.

**Fig. 1** Space infrastructure components. (Source: author)



**Table 2** Breakdown of orbital asset inventory, compiled by author with data from UCS (2019)

Total number of satellites = 2218 by 30 September 2019				
By country	United States 1007	China 323	Russia 164	Other 724
By orbit	Low 1468	Medium 132	Geostationary 562	Elliptical 56
Total estimated number of US satellites = 1007				
By character of owner	Civil 35	Commercial 620	Government 163	Military 189

## Distinguishing Characteristics of SI and CSI

The extreme technical, operational, and financial constraints under which satellite operators labor have significant results on the characteristics of CSI and the subsequent emerging risk profile, as opposed to terrestrial CI.

Firstly, their main distinguishing characteristic is, as mentioned, their low numbers. This is compounded by the size factor. While the correlation is waning with the advances in miniaturization, the larger satellites (by mass) will tend to be the most critical, because the expense needed to develop and launch them must be justified by their function and capabilities. However, according to Ambassador Sorin Ducaru, Director of the European Union Satellite Centre, speaking on 4 October 2019 in Bucharest during the International Eurodefense Conference, only half of the existing assets weigh more than 1000 kg (wet mass). Niederstrasser (2018) pegs this as the upper bounds of the smallsat category of system size, and Bryce Space and Technology (2019) confirms that around half of launched systems were in this range in 2018.

Secondly, the larger systems are more likely to be one of a kind, designed specifically for the respective mission, resulting in little interoperability with other systems or opportunities for stakeholders reliant on them to substitute for any lost capacity.

Thirdly, the cost structure and technical barriers make system replacement an expensive, long-term, and uncertain proposition, one that governments are more likely to find palatable. The CSI are also less likely to feature intermediate thresholds of functioning, where partial utility may be maintained in the event of the materialization of a risk, unlike many terrestrial CI, for whom total disruption is just one end of a long spectrum of partial disruption states (transport network carrying capacity, processing power, public services delivery rate and area coverage, partial production of energy and of goods, etc.).

These barriers are being subverted by the wider application of new technologies, like CubeSat architecture and by miniaturization, which are also an initial enabler of convergence with terrestrial CI in another important way – preponderance of ownership or operation by private entities. In Europe and the United States, the estimates of this rate are very high and vary between 60% and 85%, depending on source, and where the upper bound is set by the United States (Cellucci 2018). Bryce’s annual State of the Satellite Industry reports have noted the increase of CubeSat numbers

among launches, as well as the preponderance of nongovernmental entities (commercial, academic) among the owners. Bryce (2019) noted that 1300 smallsats (according to Bryce definitions, up to 600 kg) were launched between 2012 and 2018, of which 961 were CubeSats. And half of all of these provide commercial services, especially in remote sensing. This trend accounts for the high use of low Earth orbit, and the differences in inventory breakdown would be even starker, if orbital dynamics and atmospheric drag did not lower the mission time of such satellites.

CSI are expected to function in a very challenging security environment, featuring both natural and man-made threats, the latter divided into unintentional and deliberate. The Royal Academy of Engineering (2013) notes the high likelihood of spontaneous malfunction from environmental pressures, derived also from mass and cost constraints for the engineering of more robust systems, though this is also proceeding apace. Terrestrial CI do not generally feature such high background risk levels, since existing regulations regarding resilience from the design phase, on a sectorial and national basis, attempt to reduce the impact of background factors (geology, hydrography, etc.) or include them in decision-making regarding critical infrastructure commissioning. The space-specific threats of debris collisions and extreme space weather phenomena also significantly impact CI, while the former also presents a significant collective action failure that any emerging governance framework will have to address. Moreover, from the beginning, the US National Security Space Strategy has defined space as a "congested, competitive and contested" environment (DoD and ODNI 2011).

CSI are also interesting for their limited current range of interdependency types. Until we have arrived at the level of space industrialization and active resource exploitation, there will be very few cases of physical interdependencies, or of bidirectional dependencies.

## Critical Space Infrastructure Protection

Heino et al. (2019) argue, with regard to traditional CIP efforts, that "a severe disruption in the system can go beyond geographical, organizational, and administrative boundaries, thus activating a multifaceted set of actors whose ability to collaborate is required to restore the situation." Stakeholders will have to engage in Critical Space Infrastructure Protection (CSIP) efforts in order to improve the resilience of CSI or of the system-of-systems in which it is operating. Starting from a common definition of CIP, CSIP efforts comprise all of the programs and activities in which stakeholders will engage in order to maintain the level of functioning of Critical Space Infrastructures above a predefined threshold in case of the materialization of a threat and to minimize the casualties, material damage, and systemic impact on other CI. The stakeholders run the gamut from manufacturers of components and providers of services to the owners/operators of CSI, the competent national authorities (civilian, military), and various international or supranational organizations. The latter is the case of the EU, which administers the EU space



program, comprising the Galileo/European Geostationary Navigation Overlay Service (EGNOS) global navigation satellite system, the Copernicus remote sensing program, and the future governmental satellite communications network for EU and EU Member State government communications.

While CSIP is a subset of CIP efforts, it is important to acknowledge the differences in approach which CSIP will entail, deriving from the specific CSI characteristics, the space security environment, and the actual ability of a respective stakeholder to govern and positively impact space security outcomes. CSIP is, from the start, a very international activity which will find distinct advantages stemming from the application of global solutions to persistent issues such as space debris, frequency fratricide (already governed globally), and hardening against space weather phenomena. Countries may not have any SI and still be critically dependent on those operated under the jurisdiction of others. Few countries have full spectrum capabilities, and none of them have total space autonomy so that their society and economy are exclusively provisioned with critical space services (and, in the future, goods) by systems under their jurisdiction. However, CSIP efforts start at the national level, which is the ideal starting point for relations with the lower orders of stakeholders involved in the process. What CSIP cannot do is solve the persistent and intentional gaps in the legal and administrative framework of space, as those are contingent on the political will of major spacefaring nations to agree to bind themselves with rules, as opposed to implementing their own programs for space security governance. CSIP can offer tools, mechanisms, and activities short of political action that can lead to an understanding of security issues, their proper communication to important decision-makers and other stakeholders, and their gradual amelioration through resilience-building measures.

It is important to note that designing CSIP governance mechanisms must also take into account the possible future state of the CSI system-of-systems and its environment. This estimate is not only technological but also social, legal, political, geopolitical, and economic. Exercises in strategic foresight like the one described in *The Future of Space 2060* report released by Air Force Space Command in 2019 may hold particular significance for each organization, but they are ultimately developing scenarios for system contexts, infrastructure, and interrelationships that will determine the governance solutions necessary to maintain system viability (Air Force Space Command 2019), which is an almost exact description of complex system governance under CIP efforts.

What we can say with near certainty about the future is that we will have many more space systems in place, as well as space actors (especially private ones), that our dependence on them will have increased and new dependents will have materialized from the developing world. The potential results of the materialization of a negative event will have increased as well, maybe to the point of becoming an existential threat at systemic levels. Significant uncertainties will persist in the legal and administrative realm, as the best positioned countries to profit materially and strategically from this ambiguity will head off most efforts aimed at collective action toward positive security transformations. Just as in the steady globalization of CIP, CSIP will be an important vector for the coalescing of common concepts, definitions, toolboxes, practices, and standards, because of the previously stated need for

practitioners to cooperate because of interdependencies. The increasingly globalized private sector will act as a vector for the spread of these elements, as they will be able to cooperate with CSIP efforts and CIP efforts aimed at managing the exposure to CSI risk in each country in which individual companies are present and are regulated from a CIP perspective by the national authorities.

---

## Results from Framework Application

If we were to apply the CIP framework to space systems, we would have to be careful to keep in mind the specificities of these systems, of their operating environment, and of their threat matrix, as mentioned in the prior sections. It would also require acknowledgment that some of the elements of a CIP framework may already be under development or in place, such as a space situational awareness program.

It is important to note that CIP also influences considerations on future SI design in favor of resilience and the achievement of acceptable levels of the qualitative and quantitative indicators of resilience listed in the CIP theory section.

The application of CIP would require competent national authorities to begin an identification and designation process for CSI, based on a methodology they have developed for this purpose, in order to allocate scarce security resources to where they would have the highest impact. Owners/operators (OO) of CSI would come under the purview of the competent sectoral authority and would have to conform to regulations regarding protection measures and coordination with the other stakeholders in the national CIP system. This varies on a state-by-state basis, but it generally entails the development of an operator's security plan (OPS) for approval by the competent authority, its regular update (on a set schedule or whenever the situation calls for it), and the implementation of a communication system or structure with the liaising authority. In the European system, this is achieved through security liaison officers embedded within the infrastructure operator and the competent authority, as well as mechanisms for the sharing of relevant information.

CI operators/owners in energy, transport, and other domains would also have to take note of their dependence on CSI, apply adequate methodologies to estimate it, and factor it into their respective OPS.

A generic OPS identifies vulnerabilities, describes existing security programs, and details the ones that will be implemented, as well as the gradual and permanent measures that are instituted with every increase in the alert level.

For a CSI OO, the OPS would include not only references to background security levels but also readiness levels for expected threats such as space weather. The OO is tasked to articulate a security vision for its CSI, in order for the OPS to meet with approval from the regulator, such as plans for new satellite design policies that stress resilience through physical and electromagnetic shielding, for security through obscurity by using specially designed software and other systems, or for redundancy in the form of higher satellite counts, lower replacement times, and so on.

For an OO of an infrastructure dependent on CSI, the OPS would include its plans to mitigate the risk of disruption of critical space services. The possibilities are

varied – it may have contracts in place with alternate providers or even alternate system providers, who are not subject to cascading disruptions in the space environment (e.g., ground-based data collection as opposed to space-based remote sensing). The OO may also commit to a reduction in its dependence on CSI, though many entities have limited ability to negotiate and limit CSI risk from third parties (such as OOs of other CI on which they are dependent).

Depending on the country in question, it is possible that there are no CSI OOs within the national jurisdiction. These countries must manage their dependence on CSI without having the possibility of exerting influence to ameliorate their vulnerabilities and therefore face a slew of other challenges and uncertainties (including political) when compared to countries with partial or full spectrum space capabilities. These countries may become active in international fora (such as UN COPUOS – the Committee on the Peaceful Uses of Outer Space) and intergovernmental arrangements in order to pursue a part in collective governance efforts.

Georgescu et al. (2019, p. 272) speculated that one answer to the issue of space governance may lie in the change of incentive structure resulting from the formalization of the space governance issue, for instance, through the CIP framework. Whereas a collision in space or some other disruptive or destructive event may currently be written off as an “Act of God,” the average CI operator on Earth finds himself under greater scrutiny when disruptions occur. The CI designation system formalizes a responsibility on the part of the OO, as well as the competent authority and the ultimate coordinating authority at higher levels (the Ministry of Interior in the European model, the Department of Homeland Security in the American one). A failure of due diligence, such as inadequate security measures, exposes the OO to liability issues, whose potentially significant costs may eventually make them more accepting of the higher costs of greater security. A market-centric governance model may also emerge, where unsustainable behavior in space, with impact on the security outcomes, may also be sanctioned in an emergent manner through market mechanisms – interest rates for funding new investment or insurance premia may be lower for security-conscious actors whose systems are less prone to disruption or destruction by design or through other factors.

Given the nature of the space environment, CIP efforts must also focus on cooperation between nations, as they are starting to do also on the ground, with the emerging coordination for the protection of transborder or global infrastructure chains in energy or transport (EPCIP's efforts have been mainly in the energy and transport areas, if one looks at the list of designated ECI). By stressing the mutual dependence of countries and the security gains from having a resilient CI system-of-systems, cooperation under a CIP framework, especially between different orders of stakeholders below the political level, may have far-reaching impact.

## Principles of Resilience

As mentioned before, the application of a CIP framework seeks to increase the resilience of the system in question or of the wider CI system-of-systems. CSI would

also strive for resilience and thereby utilize the conceptual toolbox described in the previous chapter to plan for an increase in resilience. In this regard, Johnsen (2010) describes seven principles of resilience whose application to space systems may clarify the results of a CSIP framework.

Chief among these is the graceful or controlled decline, which is the result of competencies and capacities which arrest the quick decline of a system, for instance, through the prompt and efficient intervention of emergency response teams or other contingency measures. The system is also set up in such a way that the chance of catastrophic system degradation, such as a facility exploding, is minimized. Solutions may vary depending on the type of space system in question (single or constellation, for instance), but they generally rely on operators having identified key issues in the CSI functioning which may accelerate service degradation.

Key for CI resilience is also the management of margins, where operators do not just evaluate risks, but also acknowledge them when they occur, as they erode the system margins which allow a still acceptable level of functioning above the critical threshold for rapid system degradation. Systems are tested for their capacity to remain within safe operational margins, and operators use proactive indicators to measure the state of the system's margins. Such a principle may appear less applicable to space systems but one may find examples, such as the management of fuel for station keeping in the backdrop of the need to maneuver to avoid impact with debris, but also to maximize system lifespan and minimize debris creation upon mission end.

For CSIP efforts to work as a collective endeavor, they require common mental modes among the various categories of active stakeholders and *system governors*. The OOs must be able to communicate not only among themselves but also with the OOs of CI dependent on CSI and with the sectoral authorities and overall authorities, as well as the growing layer of global stakeholders, such as international institutions. This is an effective way to prevent accidents, mitigate their effects, and assimilate lessons from various disruptions.

Resilient systems are also flexible and redundant. The former is less applicable to space systems, which are generally path dependent on the specific architecture of the system in question, but flexible systems are also open to incremental improvements and improvisations, which are possible in the realm of cybersecurity, among others. The latter principle of resilience, redundancy, is also problematic with regard to the space component of a CSI, though it may be applicable elsewhere. Having reserves and multiple systems running in parallel are workable ideas, but one should remember that redundancy is also another source of complexity, which is a source of risks such as common cause failures. Diversity of systems, as a subset of flexibility, is also an option.

The issue of complexity is a permanent concern for CIP efforts, as its rise obscures interactions between systems that may result in new risks, vulnerabilities, and threats or paths for cascading disruptions. The reduction of complexity is, therefore, a common security concern, though it often develops into the management of the growth rate of complexity, since the prioritization of economic growth, efficiency, and development is a leading cause of complexity buildup. Space systems

are also subject to this “iron law,” with systemic trends indicating that complexity will increase in the CSI operating environment through the rise in new systems, the rise in orbital crowdedness, the growing number of interactions between systems and system components, and, last, but not the least, the growing complexity of the individual assets themselves, which are on their way to integrating AI, blockchain, and other developments. An often-overlooked source of complexity when it comes to technological assets is also the organization behind its operation. Generally, a system becomes less complex as it reduces the possibility of feedback loops, as it segregates functions and creates direct lines of information with unique pathways for each.

Under these conditions, the most that CSIP practitioners may hope for is the reduction in system couplings, or the rate of transmission of disruption from one system or system component to another. For instance, fossil fuel-based power generation facilities may reduce their coupling with the mining asset or the transport infrastructure by having reserves on hand, granting autonomy during the initial phases of a crisis. With regard to CSI, we may consider reducing the rate of propagation of cyber threats, but other examples are possible. Overall, systems that reduce couplings are flexible in their operating manner and in the resources they use, and they have delayed or non-sequential functioning compared to their upstream CI influencers.

Johnson and Gheorghe (2013) added two more principles for resilience. The first is the reduction in system fragility, which is an endogenous factor in the system, and the opposite of vulnerability, which is an exogenous factor affecting the system. One may find many instances in the functioning of a CSI which may be assimilated to a state of fragility, but an often-overlooked factor is the organization of the OOs and, for instance, their financial vulnerabilities, cost structures, openness to subversion from abroad, etc.

The second, drawing from the financial sector, is the concept of anti-fragility, which is the quality of a system to be strengthened by the repeated application of small stressors. The classic example is of a forest experiencing regular small fires and then ceasing to do so, following human intervention. The accumulation of plant matter makes the inevitable future fire much more dangerous and stronger when compared to the strength of the smaller, regular fires. We may argue that this quality is also present in space systems, whose challenging security environment has led prospective developers toward increased robustness, within the financial and mass constraints of the launch systems. Baker et al. (2008) have noted that the various coronal mass ejections and other space weather phenomena that have been analyzed do not compare to the potential of the largest solar storm ever recorded (the Carrington Event – 1859), but they are sufficient to produce damage both in orbital and ground-based assets. However, no episode has, so far, been an existential threat, and this has also spurred research into hardening systems and into the development of early warning systems and mitigation measures. The system, overall, becomes stronger than it would have been under ideal conditions, when a Carrington Event-level solar storm would have much graver consequences (Hapgood and Thomson 2010).

## Complex System Governance

As mentioned in the description of the CIP framework, CSG is an emerging field at the intersection of several disciplines that has the potential to resolve some of the issues inherent in the manner in which the governance of space systems has developed over time –piecemeal and self-organized, based on gradual accumulation. This organic development is sometimes satisfactory, but it often leaves important gaps in the space governance framework which CSG is uniquely positioned to address. According to Keating et al. (2014), CSG is the design, execution, and evolution of the metasystem functions necessary to provide control, communication, coordination, and integration of a complex system. Metasystems “are sets of related functions which only specify ‘what’ must be achieved for continuing system viability (existence), not specifying ‘how’ those functions are to be achieved” (Keating and Katina 2016). These include system identity, system context, strategic system monitoring, system development, learning and transformation, environmental scanning, system operations, operational performance, information, and communications. It is beyond the scope of this chapter to engage in detailed explanations of the underpinning of CSG, but it suffices to say that CSG focuses on system viability and purposeful design in that direction, through a loop of system analysis (*initialization*), readiness levels assessment, and governance development (Keating and Bradley 2015).

In the absence of a purposeful design, Georgescu et al. (2019, p. 323) diagnose the existence of *system drift*, a state in which the system accrues unintended consequences. These consequences are also the result of the emergent behaviors and phenomena of the system which could not necessarily have been anticipated from the analysis of its individual components. The deviations from healthy system conditions are termed “pathologies” (Keating and Katina (2016) mentioned 53 identified pathologies), and they result from a violation of one or more of the metasystem functions. They degrade system functioning to the point where viability becomes in doubt. Identifying these pathologies and resolving them is necessary for system health.

From a CSG perspective, the governance of CSIP has four key issues. The first is the increased complexity in design, execution, and development. The second and third are the importance of including a wide range of considerations from multiple fields in the development process while maintaining a design which offers direction, oversight, and accountability. Lastly, the stakeholders involved should have different worldviews and must participate voluntarily.

Many of the challenges in Fig. 2 will be present in the complex system represented by the space infrastructures and the interactions with their environment or the wider system-of-systems in which space infrastructures are embedded.

From the perspective of CSG, its application to CSI starts with the clarification and structuring of the problem matter around critical systemic issues from across the spectrum of relevant problems, from political to economic and strategic. It continues by mapping the CSI governance metasystem, with its contexts and the various interrelationships, which will allow for the discovery of profound systemic problems



**Fig. 2** The complex system problem domain and its five challenge fields for practitioners (Georgescu et al. 2019, p. 322)

once the practitioner has applied different CSG-specific methods and tools. These steps are done through extensive modeling and simulation, which relies on the systematic disassembly of the issues in the initial stage. Since “the map is not the territory,” we must be careful with the biases and mistakes of our base definitions and functions. Following this, governance options can be formulated, designed, modeled, and tested before execution in the real world where they will hopefully increase system viability.

For instance, one important issue that affects the viability of the CSI complex system is the issue of space debris. The inadequate development of space governance in this field has led to a “tragedy of the commons” type situation, where a critical asset and resource (orbital bands) is steadily deteriorating. The risks of collision in these areas become ever higher (Salter 2015) and inflict steadily higher damages on the collective of users and possibly triggering also a cascading collision event once past a certain critical threshold (the so-called Kessler syndrome). This is a governance failure because system viability is imperiled and the makeup of the governance structure does not incentivize self-restraint in the creation of debris; does not punish the act of polluting, even deliberate pollution as part of anti-satellite weapon tests; and does not foster the financial preconditions for designing and deploying debris cleanup measures.

Following the CSG process outlined above, we might find something similar to the system briefly outlined in the previous section, where financial incentives are created for sustainable behavior, or something else entirely.

## Conclusions

Over the course of this chapter, we have argued in favor of space systems as a new CI category and the potentially significant security benefits stemming from the application of the CIP framework in order to increase the resilience of CSI and of the societies which are critically dependent on them.

The significant advantage of the CIP framework is that it is already a debated and developed field, with significant impact on security policy and the legislative/administrative frameworks for security in the United States, the European Union Member States (as well as the EU itself), and other countries. Extending it to the space environment has the potential to improve security outcomes and to address some of the gaps stemming from the organic development of the space security governance framework under the unique conditions of the space security environment. Critical Infrastructure Protection provides a comprehensive framework for the management of key infrastructures, assets, and resources on which individual countries or the global community depends. Since space systems are already an acknowledged component of the existing critical infrastructure domains, the CSI concept is a natural outgrowth.

To sum up, the CIP framework provides tools and concepts with which to analyze space security and describe the relationships formed with terrestrial infrastructures. It is also a gateway to an extant governance framework which is in use at American and European levels, both for individual nations and collectively. It also provides a coherent vision for a holistic understanding of security, in which space security is not cordoned off into its own field, but is integrated in the wider security domain as befits the reality of the complexity of the critical infrastructure system-of-systems. The CIP framework has been working toward alleviating the impact of trends in terrestrial CI which are also present among space systems, most notably the growing rate of ownership by private entities of prospective CSI, but also the potential of counterspace operations within the hybrid warfare becoming the new normal among rival states (Robinson et al. 2019). In addition, the recent developments in the CIP field, such as complex system governance, are also applicable to CSI.

For these reasons, the concept of CSI and all that derives from it provides a useful perspective and roadmap for improving space security or at least mitigating the security impact of current space sector dynamics.

---

## References

- Air Force Space Command (2019) The Future of Space 2060 and Implications for U.S. Strategy: Report on the Space Futures Workshop, 5th, Sept 2019. <http://www.spaceref.com/news/viewsr.html?pid=52822>
- Baker D, Balstad R, Bodeau JM, Cameron E, Fennell JF, Fisher GM, Forbes K, Kintner P, Leffler L, Lewis W, Reagan J, Small A, Stansell T, Strachan LS (2008) Space Weather Events – Understanding Societal and Economic Impacts: A Workshop Report, Space Studies Board,



- National Research Council, ISBN 10: 978-0-309-13811-6, available online at <http://asp.colorado.edu/home/wp-content/uploads/2011/07/lowres-Severe-Space-Weather-FINAL.pdf>
- Bryce Space and Technology (2019) Smallsats by the numbers 2019, [Online] Available at [https://brycetech.com/downloads/Bryce\\_Smallsats\\_2019.pdf](https://brycetech.com/downloads/Bryce_Smallsats_2019.pdf)
- Bucoveţchi O, Georgescu A, Badea D, Stanciu RD (2019) Agent-based Modeling (ABM): support for emphasizing the air transport infrastructure dependence of Space systems. *Sustainability* 11 (19):5331
- Cellucci T (2018) Perspective: Innovative Public-Private Partnerships Help Secure Critical Infrastructure, published by the National Security Today, 27 Nov 2018. <https://www.hstoday.us/subject-matter-areas/infrastructure-security/perspective-innovative-public-private-partnerships-accelerate-technology-and-secure-critical-infrastructure/>
- Department of Defense, Office of the Director of National Intelligence (2011) National Security Space Strategy Unclassified Summary. Washington DC, <https://www.dni.gov/index.php/newsroom/reports-publications/reports-publications-2011/item/620-national-security-space-strategy>
- European Commission (2008) Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2008:345:0075:0082:EN:PDF>
- Eusgeld I, Nan C, Dietz S (2011) “System-of-systems” approach for interdependent critical infrastructures. *Reliab Eng Syst Saf* 96(6):679–686. <https://doi.org/10.1016/j.res.2010.12.010>
- Georgescu A, Gheorghe A, Piso M-I, Katina PF (2019) “Critical Space infrastructures: risk, resilience and complexity”, topics in safety, risk, reliability and quality, series 36, eBook ISBN 978-3-030-12604-9. <https://doi.org/10.1007/978-3-030-12604-9>. Springer International Publishing
- Gheorghe A, Schläpfer M (2006) Critical infrastructures: ubiquity of digitalization and risks of interdependent critical infrastructures, *Systems Man and Cybernetics 2006*. SMC '06. IEEE international conference, vol 1, pp 580–584
- Gheorghe AV, Vamanu DV, Katina PF, Pulfer R (2018) Critical infrastructures, key resources, key assets. Risk, vulnerability, resilience, fragility, and perception governance, topics in safety, risk, reliability and quality, series 34, eBook ISBN 978-3-319-69224-1. <https://doi.org/10.1007/978-3-319-69224-1>. Springer International Publishing
- Haggood M, Thomson A (2010) Space weather. Its impact on earth and implications for business, Lloyd's 360 risk insight briefing, available online at [https://www.lloyds.com/~media/lloyds/reports/360/360-space-weather/7311\\_lloyds\\_360\\_space-weather\\_03.pdf](https://www.lloyds.com/~media/lloyds/reports/360/360-space-weather/7311_lloyds_360_space-weather_03.pdf)
- Heino O, Takala A, Jukarainen P, Kalalahti J, Kekki T, Verho P (2019) Critical infrastructures: the operational environment in cases of severe disruption. *Sustainability* 11(3):838. <https://doi.org/10.3390/su11030838>
- Helbing D (2013) Globally networked risks and how to respond. *Nature* 497(7447):51–59. <https://doi.org/10.1038/nature12047>
- Johnsen S (2010) Resilience in risk analysis and risk assessment. In: Moore T, Sheno S (eds) Critical infrastructure protection IV – fourth annual IFIP WG 11.10 international conference on critical infrastructure protection. IFIP Advances in Information and Communication Technology series (311), p. 215–227. Washington DC, SUA: Springer, ISBN 978-3-642-16806-2
- Johnson J, Gheorghe G (2013) Antifragility Analysis and measurement framework for systems of systems. *Int J Disaster Risk Sci* 4(4):159–168
- Jonkeren O, Ward D, Dorneanu B, Giannopoulos G (2012) Economic impact assessment of critical infrastructure failure in the EU: a combined systems engineering – inoperability input-output model. Joint Research Centre, 20th international input-output conference, Bratislava. <https://www.semanticscholar.org/paper/Economic-impact-assessment-of-Critical-failure-in-A-Jonkeren-Ward/8682d0ef92243115196a66651f3d86483e37b3d>
- Keating CB, Bradley JM (2015) Complex system governance reference model. *Int J Syst Syst Eng* 6 (1/2):33. <https://doi.org/10.1504/ijss.2015.068811>
- Keating CB, Katina PF (2016) Complex system governance development: a first generation methodology. *Int J Syst Syst Eng* 7(1/2/3):43–74. <https://doi.org/10.1504/ijss.2016.076127>

- Keating CB, Katina PF, Bradley JM (2014) Complex system governance: concept, challenges, and emerging research. *Int J Syst Syst Eng* 5(3):263–288
- Linkov I, Bridges T, Creutzig F, Decker J, Fox-lent C et al (2014) Changing the resilience paradigm. *Nat Clim Chang* 4:407–409
- Niederstrasser C (2018) Small launch vehicles – a 2018 state of the industry survey, SSC18-IX-01, 32nd Annual AIAA/USU conference on small satellites, Northrop Grumman Corporation, publisher: Utah State University Research Foundation (USURF). <https://digitalcommons.usu.edu/cgi/viewcontent.cgi?article=4118&context=smallsat>
- OECD (2016) Space and innovation. OECD Publishing, Paris. <https://doi.org/10.1787/9789264264014-en>
- OECD (2019) The Space economy in figures: how Space contributes to the global economy. OECD Publishing, Paris, available at <https://doi.org/10.1787/c5996201-en>
- Perrow C (1999) Normal accidents: living with high-risk technologies. Princeton University Press. isbn:9781400828494
- Pescaroli G, Alexander D (2016) Critical infrastructure, panarchies and the vulnerability paths of cascading disasters. *Nat Hazards* 82(1):175–192. <https://doi.org/10.1007/s11069-016-2186-3>
- Robinson J, Robinson R, Davenport A, Kupkova T, Martinek P, Emmerling S, Marzorati A (2019) State Actor Strategies in Attracting Space Sector Partnerships: Chinese and Russian Economic and Financial Footprints, Prague Security Studies Institute, Prague, available online at: [http://www.pssi.cz/download/docs/686\\_executive-summary.pdf](http://www.pssi.cz/download/docs/686_executive-summary.pdf)
- Rockefeller Foundation, Arup Development Group (2014) The City Resilience Index. <https://www.arup.com/perspectives/themes/cities/city-resilience-index>
- Royal Academy of Engineering (2013) Extreme space weather: impacts on engineered systems and infrastructure, ISBN 1-903496-95-0, designated (RAENG, 2013), available at <http://www.raeng.org.uk/publications/reports/space-weather-full-report>
- Salter AW (2015) Space debris – a law and economics analysis of the orbital commons, Mercatus Center, George Mason University, USA, available at <https://www.mercatus.org/system/files/Salter-Space-Debris.pdf>
- Setola R, Luijff E, Teocharidou M (2017) Critical infrastructures, protection and resilience. In: Setola R, Rosato V, Kyriakides E, Rome E (eds) *Managing the complexity of critical infrastructures: a modelling and simulation approach*. Studies in systems, decision and control, vol 90. Springer open, ISBN: 978-3-319-51042-2/978-3-319-51043-9, <https://doi.org/10.1007/978-3-319-51043-9>
- The White House (1998) Presidential Decision Directive/NSC-63 (as PDD-63), Washington DC. <https://clinton.presidentiallibraries.us/items/show/12762>
- Union of Concerned Scientists (2019) UCS Satellite Database, accessed 12 Oct 2019. <https://www.ucsusa.org/resources/satellite-database>
- Vugrin E, Wahren D, Ehlen M (2011) A resilience assessment framework for infrastructure and economic systems: quantitative and qualitative resilience analysis of petrochemical supply chains to a hurricane. *Process Saf Prog* 30(3):280–290. <https://doi.org/10.1002/prs.10437>



Stefano Zatti

## Contents

Introduction: The European Space Agency and Its Missions .....	246
A Security-Flavored Space .....	246
Hacking in Space: Astro-Hackers? .....	247
Motivations of Attackers .....	250
Threats and Countermeasures .....	251
End-to-End Cybersecurity .....	254
Countermeasures Related to the Information Assurance Properties .....	255
Tele-Commands .....	255
Telemetry .....	255
Payload Data .....	256
ESA's Own Approach to Mission Security .....	257
Mission Categories and Security Profiles .....	259
Conclusions: New Space, New Cyber Threats! .....	262
References .....	262

## Abstract

Space-based systems play an important role in our daily life and business. The evolution of our well-being is likely to rely on the use of space-based systems in a growing number of services or applications that can be either safety-of-life critical or business and mission-critical. The security measures implemented in space-based systems may turn out to be insufficient to guarantee the information assurance properties, namely, confidentiality (if required by the data policy), availability and integrity of these services/applications, as well as authenticity and non-

---

Stefano Zatti has retired.

---

S. Zatti (✉)

European Space Agency (ESA) - Security Office, Frascati, Italy

e-mail: [Stefano.Zatti@gmail.com](mailto:Stefano.Zatti@gmail.com)

repudiation. The various types of possible cyberattacks on space segments, ground stations, and control segments are getting increasingly visible and have been indeed frequent. What to do in order to counter such occurrences is less obvious and needs to be addressed with priority and a whole new family of countermeasures. This paper will first introduce ESA and its constituency, and then it will address the security-specific aspects of its space missions. Threats specific to the different types of missions from the cyberspace will be presented, and possible countermeasures will be analyzed. The motivations that may induce some offenders to cause damage to space missions will be then examined. A categorization of the different types of space missions will then lead to the proposal of creating different protection profiles, to be respectively implemented at increasing degrees of sophistication for the different mission categories.

---

## Introduction: The European Space Agency and Its Missions

The European Space Agency, ESA, was founded in 1975 by merging two existing launch and space research organizations, with the aim expressed in Article 2 of the ESA Convention: “To provide for and promote, for exclusively peaceful purposes, cooperation among European states in space research and technology and their space applications.” Composed of 22 member states, with eight major sites/facilities in Europe and a large number of ground stations around the earth, providing attractive jobs to about 2200 staff, ESA has in the course of its lifetime designed, tested, and operated in flight over 80 satellites.

---

## A Security-Flavored Space

Although they are conceived, designed, and operated for peaceful purposes, the space missions of ESA can indeed present security aspects and address security elements. The different critical elements of space missions can influence the level of sensitivity and consequently the level of threats that each one of those space missions has to face. In particular, the following aspects of “security from space” have been highlighted by the ESA Council as critical for the benefit of European citizens, leading to the development of specific missions to address those.

### *Security on Earth:*

- **Disaster management:** the use of space systems to support natural disaster management, such as climate change or earthquakes
- **Critical infrastructures protection:** space-based applications and technologies used for the safety and security of critical infrastructures
- **Transportation and logistics:** space-based solutions to support transportation on land, air, and water

- **Energy:** space-based technical contributions to the management of energy production and supply
- **Agriculture and water:** space-based applications in support of the 2030-agenda formalized as the Sustainable Development Goals, in particular no. 6 (clean water), 2 (zero hunger), and 15 (life on land)
- **Surveillance (air, sea, land, space):** space surveillance in support of national and international programs on air, sea, land, and space
- **Humanitarian crisis support** and emergency rescue tasks
- **Migration and border control:** space-based applications in support of grand challenges such as migration and border control
- **Public safety (including civil protection)**

#### *Security in Space:*

- **Space situational awareness:** real-time information of the status (position, direction, speed) of specific objects in space
- **Near-earth objects:** asteroids, meteorites, in the vicinity of our planet
- **Space weather:** phenomena outside the atmosphere that can affect terrestrial infrastructures, like solar winds and electric power grids
- **Satellite tracking:** knowledge of position and trajectory and speed of man-made objects through active and passive observation and tracking

It is clear that when dealing with such subjects that the space missions can create interest in malevolent individuals or organizations to have an impact on them in different ways (see section later). Having such sensitive scope, the space missions require therefore that the responsible authorities establish a set of measures to protect them from adverse effects, encompassing both the assets composing them (space and ground) and the data they provide.

---

## **Hacking in Space: Astro-Hackers?**

We introduce first the definition of a few basic concepts that are necessary in the broad context of addressing threats and analyzing risks. ISO 27005 (Information Technology—Security Techniques—Information Security Risk Management 2018) defines “threat” as “A potential cause of an incident that may result in harm of systems and organization,” whereas the Consultative Committee on Space Data Systems (CCSDS) 350.8-G-1 (Information Security Glossary of Terms 2012)) defines “risk” as “Possibility that a particular threat will adversely impact a system by exploiting a particular vulnerability.”

A threat can be generated by human or nonhuman sources and can be intentional or unintentional. All threat agents attempt to do harm against a physical or virtual resource or asset. In case that the resource has one or more vulnerabilities, it can potentially be exploited by a threat agent, resulting in a compromise of the properties of information assurance (IA) of the system, namely, confidentiality, integrity, or

availability (traditionally, C-I-A), plus authenticity or non-repudiation. In particular, loss of confidentiality will result in unauthorized disclosure of information; loss of integrity will result in unauthorized modification or destruction of information; loss of availability will result in a loss of access to critical resources; lack of authenticity will result in doubts of the sources and the genuine nature of the available information. Lack of non-repudiation will result in uncertainty of transmission and/or reception of particular pieces of information. Overall, the loss of information assurance might result in harm to an agency's operations, assets, or individuals.

Computer systems are typical targets of threats given the attractive nature of the information they contain and make offer to the majority of legitimate users, while they often suffer from a number of vulnerabilities. The National Institute of Standards and Technology's (NIST) Special Publication 800-12 (An Introduction to Computer Security—The NIST Handbook 1995) states that:

Computer systems are vulnerable to many threats that can inflict various types of damage resulting in significant losses. This damage can range from errors harming database integrity to fires destroying entire computer centers. Losses can stem, for example, from the actions of supposedly trusted employees defrauding a system, from outside hackers, or from careless data entry clerks.

The pervasive interconnectivity of networks and the ever-increasing dependency of industrial, commercial, and scientific activities, including space missions, on information technology and communications, create a whole new dimension to the threats that can affect a space mission. In the past, in order to reach a satellite in orbit to threaten its functions, in fact, it would have been necessary for the adversary to build or possess an infrastructure to generate and send tele-commands to the spacecraft, an expensive and massively complex endeavor. In the most brutal case, the attacker would have to gain physical access to the ground infrastructures to raise havoc to the people and infrastructures located therein, thus gaining the capability to affect the spacecraft. Nowadays, via the pervasive nature of the access networks all interconnected through the Internet, it is sufficient for a hacker to tamper with and bypass the existing protection measures simply while sitting in their own offices or homes. This is not just science fiction: there have been several publicly documented events including the cases described below:

- In 1998, the German-US ROSAT space telescope inexplicably turned toward the Sun, irreversibly damaging a critical optical sensor, following a cyber-intrusion at the Goddard Space Flight Center of NASA in the USA ([HTTPS://EN.WIKIPEDIA.ORG/WIKI/ROSAT](https://en.wikipedia.org/wiki/ROSAT)).
- On October 20, 2007, Landsat 7 experienced 12 or more minutes of interference. Again, on July 23, 2008, it experienced other 12 min of interference. The responsible party did not achieve all steps required to command the satellite, but the service was disturbed.(Satellite Services and Interference-the Current Situation).
- In 2008, NASA EOS AM-1 satellite experienced two events of disrupted control: in both cases, the attacker achieved all steps required to command the satellite but did not issue commands.

These cases made the news, as shown in Fig. 1. ([HTTPS://WWW.DAILYMAIL.CO.UK/NEWS/ARTICLE-2055311/HACKERS-INFILTRATE-US-SATELLITES-TAKEN-COMPLETE-CONTROL-ACHIEVING-STEPS-REQUIRED-COMMAND-SATELLITE.HTML](https://www.dailymail.co.uk/news/article-2055311/hackers-infiltrate-us-satellites-taken-complete-control-achieving-steps-required-command-satellite.html)).

ESA itself has not been immune to attacks, of course. As recently as December 2015, an attack by Anonymous has compromised a large number of accounts of external users who were accessing the targeted service to gather ESA mission data that was already openly available to the public but required preregistration (Fig. 2). The fact that the service was entrusted to a third party did not actually mitigate the damage, as proper protection measures should have been imposed on the provider by the ESA customer, according to the prevalent rules. Although the data compromised was not highly relevant, due to the open data policy, the reputation of the organization was damaged by the occurrence. Moreover, all affected identities had to be urgently contacted and informed, to avoid that the compromised identities could be used by the attackers to access other sites, increasing the impact and potential damage. “A group of hackers operating under the Anonymous banner hacked the European Space Agency (ESA) and leaked the data for no reason other than for “lulz.” Over 8000 people will not find anything amusing about the breach since their names, email addresses and passwords were posted in one of three data dumps on JustPaste.it” (Anonymous Hacks The European Space Agency; Attackers Hack European Space Agency, Leak Thousands Of Credentials 'For The Lulz).

Some more cases are presented below, organized by the categories of the missions that were affected (Fig. 3).



Fig. 1 Press report on US satellite hacking



## Anonymous Hacks European Space Agency, Releases Data Online

They did it for the 'lulz.'

By **Adam Toobin** on December 14, 2015

Filed Under **Cyberwarfare**

**A**fter a series of high-profile attacks on targets potentially worth attacking — ISIS, the KKK, and Donald Trump — Anonymous, the online hacking collective, reaffirmed its commitment to chaos this weekend when it broke into the database of the European Space Agency and released names, emails, and passwords of officials online. There's no particular reason to think the hack put anyone at risk, but it represents an inconvenience for an agency that has better things to do than field calls from hacker aspirants (think: TK).



What could have possessed them to go after a target so seemingly undeserving compared to their other recent marks? According to *HackRead*, a 'representative' of Anonymous declared:

BECAUSE XMAS IS COMING AND WE HAD TO DO SOMETHING FOR FUN SO WE DID IT FOR THE LULZ.

**Fig. 2** Anonymous hacks ESA data servers

## Motivations of Attackers

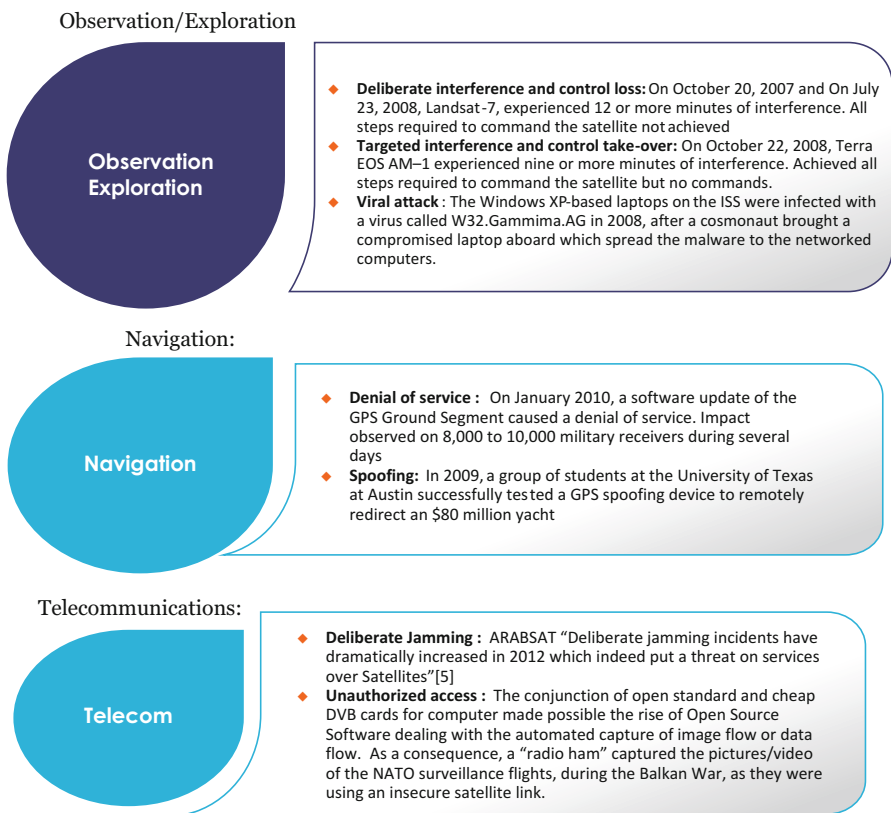
What are motivations for potential attackers to expend effort and undertake risks to damage space systems? The financial gain in the cases we have presented is nonexistent. Other possibilities for the motivations, as well as what could be the characteristics of such perpetrators in a broader spectrum of cases, are addressed in the following.

One possible motivation can be the search of technological information by commercial or institutional competitors, possibly by means of third parties: the knowledge gained by hacking equipment or data could be used to bridge technological gaps and gain competitive advantages in the space arena.

Cybercriminals could insert themselves in this race by gathering information and technical details that they could sell to interested parties for some sort of financial advantage. This would require considerable technical skills including ability to do reverse engineering, to make sense out of the gathered information.

Employees of the organization could be the sources of additional threats, seeking some sort of revenge for perceived mistreatment or simply by unwittingly creating havoc with their negligent behavior. Insider threats are indeed often referred to in the literature as major sources of hacking problems.





**Fig. 3.** Cases of satellite hacking organized by mission types

Given the very high resonance of space-related news, some hackers could turn out to be politically or socially motivated to hamper space mission, thus gaining a high visibility, like the case of the Anonymous attack to ESA mentioned before. Even worse, some terrorists, driven by motivations of political or religious nature, may want to penetrate space-based infrastructures and impact the services they provide to the broad user community, to cause cascaded damage to any other critical infrastructures of different nature, with potentially disastrous impact (e.g., health, energy, water, transportation, telecommunications).

## Threats and Countermeasures

The infrastructures supporting all space missions can be in general characterized by a *ground segment*, a *space segment*, and a *control segment*. The control segment is used by the mission controllers, who issue tele-commands (TC) that via the ground segment can be uploaded all the way up to the space segment, a set of spacecraft that circles in

space at possibly different altitudes, depending on the mission type. In the other direction, the spacecraft send back to Earth messages containing housekeeping telemetry (HKTM) to indicate the status of the various instruments and on-board parameters, and the payload, that is the *raison d'être* of the mission and can be constituted by very large amounts of data (like in the case of Earth observation missions).

The threats that can affect a spacecraft in orbit can be characterized by the different ways that adversaries can use to tamper with the tele-commands that are normally sent from the control center to the spacecraft to perform specific mission-related actions, as well as with the data that returns to Earth, be it either payload related to the mission or housekeeping telemetry that informs ground control of the status of the instruments on board (Security Threats against Space Missions, 2015).

In a recent talk at the RSA Conference on cybersecurity, for example, Bill Malik, VP of Infrastructure Strategies at Trend Micro, calls the range of vulnerabilities exposed on satellites “astonishing” ([HTTPS://WWW.EXTREMETECH.COM/EXTREME/287284-HACKING-SATELLITES-IS-PROBABLY-EASIER-THAN-YOU-THINK](https://www.extremetech.com/extreme/287284-hacking-satellites-is-probably-easier-than-you-think)). Malik stresses the need for satellite design to incorporate security at the most basic levels, by implementing an appropriate set of countermeasures, as we will see in the following.

When addressing the need to protect space missions and develop the appropriate set of countermeasures, a systematic approach based on risk analysis methodology must be followed, as described by the author in a paper that summarizes the outcome of two studies commissioned by ESA in 2014 to address the specific situation of its current missions (Del Monte and Zatti 2015). The risk assessment methodology described in the paper is structured in four phases:

- *The first phase: Cyber threat analysis* to define the context of the analysis, by defining and modeling the space missions and considering all the possible threats they can be subject to, with particular attention to the new generation of cyber threats, as described in the following
- *The second phase: Identification and assessment of vulnerabilities* to identify the potential existing vulnerabilities of the assets of the space mission classes and to define elementary threat scenario
- *The third phase: Identification and assessment of risks* to assess identified vulnerabilities, to evaluate the related risks, and to build attack trees based on the space mission architectures
- *The fourth and final phase: Definition of the necessary measures to counteract the threats* and address the risk as defined in the previous phases, resulting in a set of recommendations and a mitigation plan

There are events that, when happening, could have a significant impact on the mission, performance, economics, human safety, data loss or compromise, or even the total loss of the mission. These events can be classified in a hierarchy based on what are the most feared events among them, on which a mission planner has to put extra effort by devising appropriate countermeasures in order to decrease the chances of suffering the resulting damage.

Each category of missions has its own most feared events; we will consider in this paper only those most frequent or likely and potentially harmful, among all the feared ones.

- *Unauthorized operation of satellite/launcher/spacecraft/ground facilities*

This is one of the most feared threats among the flight control team members and possibly one of the easiest ones to achieve.

Satellites are usually designed with an on-board and autonomous failure detection and recovery system, which upon detection of any failure on-board they will configure themselves into a safe position, awaiting for ground to investigate. So, if someone managed to send commands to cause any harm, the satellite will go into a safe mode by itself before the damage was irreversible. In this sense, the damage could be the loss of science, service, and money. However, there are circumstances where the mission could be lost. Those cases could occur:

- If someone knows the spacecraft design and its operations very well, it could generate a sequence of commands that would really cause the end of the mission, like de-orbiting the satellite or causing a failure of the on-board communications system. The places where someone could introduce commands are via the mission planning system, the flight dynamics system, the mission control system, or directly at the telemetry and command system located at the ground stations.
- If someone manages to command the satellite for a longer period, even after the satellite has gone to safe mode, it could also create an on-board failure to end of the mission.
- The receivers that live in spacecraft which are flying in orbits below geostationary (GEO) are sensitive to the received radiofrequency signal power. If the ground station uplink amplifier was manipulated to uplink with a higher power than the allowed one, and then the receiver could be broken, meaning the end of the mission. Usually, the spacecraft have two receivers, but as they are working in hot redundancy, if this event occurred, it could end with both receivers at once. Manipulation of the uplink amplifiers can be done through the hardware itself, via the ground station jobs generated at the control center and sent to the station via ftp, via the ground station jobs once stored at the station computer of the ground station.

The launch is a very critical phase of the mission. If someone managed to insert a wrong command into the launch-automated sequence to inject a failure on any of the critical activities, like the separation sequence, or the burns needed, then it could cause the loss of the launcher and of the spacecraft carried inside.

- *Unavailability of the communications for tele-commands and telemetry during critical maneuvers*

There are different activities that are considered critical, those ones that have an impact on the success of the overall mission. Typically, these activities consist on

different type of maneuvers: launch and early orbit phase (LEOP) maneuvers, planetary swing/fly-by, trajectory correction maneuvers, in-orbit insertion maneuvers, and collision avoidance maneuvers, among others. During the execution of any of these maneuvers, it is very important to maintain contact with the spacecraft or the launcher in order to get real- or near real-time ranging and Doppler shift measurements.

- *Unavailability of critical services for medium or large periods of time*

The HVAC systems (heating, ventilation, and air conditioning system) provide the air quality to the human spaceflight vehicles. The maintenance of the atmosphere aboard the spacecraft is critical, not only for its habitability but also for its function. If this system failed, the spacecraft cabin will get contaminated with so many chemical contaminants that it will be impossible to live there.

- *Equipment destruction or theft*

The most feared and disruptive of all events is the loss of the whole equipment, by destruction or theft, with the prospect of a total prejudice to the mission.

Analyzing more in depth the ways such events can be determined, it must be realized that the syntax of the tele-commands is known and common to many missions. An intruder can thus prepare her own attack by counterfeiting the tele-commands in proper syntax, but she has then to upload them to the spacecraft for execution. In the past, such action was not simple to perform, requiring access to space via complex and expensive ground infrastructures, not easily available and not easily accessible. However, nowadays, given the very widespread and ever-increasing connectivity of operational networks with public networks, the intruder can gain access to the ground infrastructures by hacking their access control at the network boundaries, and they find a way to issue commands to the spacecraft, affecting its functionality.

Likewise, the downward stream can be affected by capturing the telemetry (that can provide important indications on the state of the spacecraft and its instruments, as well as the payload, affecting the confidentiality and the availability of the data to the intruder and further on to other parties).

---

## **End-to-End Cybersecurity**

In order to ensure the proper protection of all the assets related to space missions, including the segments described above, material and human, as well the mission data, it is necessary to tackle the various aspects of security as a process that spans all components and all phases, in an end-to-end fashion.

This implies the consideration of the security pillars and the respective counter-measures, as follows.

- Physical: zoning, access control for data centers, perimeter and internal fencing
- Personnel: vetting, clearances, building trust in employees, peer control
- Information protection: classified vs unclassified data and parameters
- Information assurance (IA) properties and respective ways to ensure them:
  - Confidentiality – encryption
  - Integrity – media access control (MAC)
  - Availability – redundancy
  - Authenticity – identity management, cross check, access control, signature of data
  - Non-repudiation – notarization, certificates

---

## Countermeasures Related to the Information Assurance Properties

The following analysis will provide insight of the specific countermeasures that must be enacted to counteract the respective threats, to be applied to tele-commands (ground to space), telemetry (space to ground), and payload data (space to ground too). The quoted algorithms are introduced and well explained in reference (CCSDS Cryptographic Algorithms 2014).

### Tele-Commands

*TC Availability:* a combination of spread spectrum, firewall and autonomy techniques, high-power uplink margins, and diversity of the sites of the telemetry and tele-command stations seem appropriate to reduce the risk down to an acceptable level.

*TC Integrity:* integrity of individual commands can be achieved by appending an integrity check value (ICV) in a manner similar to the way a digital signature is appended. To ensure that it is not modified or corrupted, the ICV is often keyed (e.g., a keyed hash), or the ICV value can be encrypted using a symmetric encryption algorithm (e.g., AES).

*TC Authentication:* use encryption of the messages at the segment level, with a block cipher-based message authentication code (MAC).

*TC Confidentiality:* at packet level, use Advanced Encryption Standard (AES) algorithms in cipher feedback mode (CFB), output feedback mode (OFB), or in counter mode of operations (CTR), the latter recommended by CCSDS.

*TC Sequencing (Anti-replay):* insert in the command an integrity-checked progressive sequencing number based on a counter.

### Telemetry

To ensure *housekeeping telemetry confidentiality* at virtual channel level, use Advanced Encryption Standard (AES) algorithms in cipher feedback mode (CFB),

output feedback mode (OFB), or in counter mode of operations (CTR), the latter recommended by CCSDS.

*Housekeeping telemetry* Integrity can be obtained by appending an ICV in a similar manner to that used for tele-commands (see above).

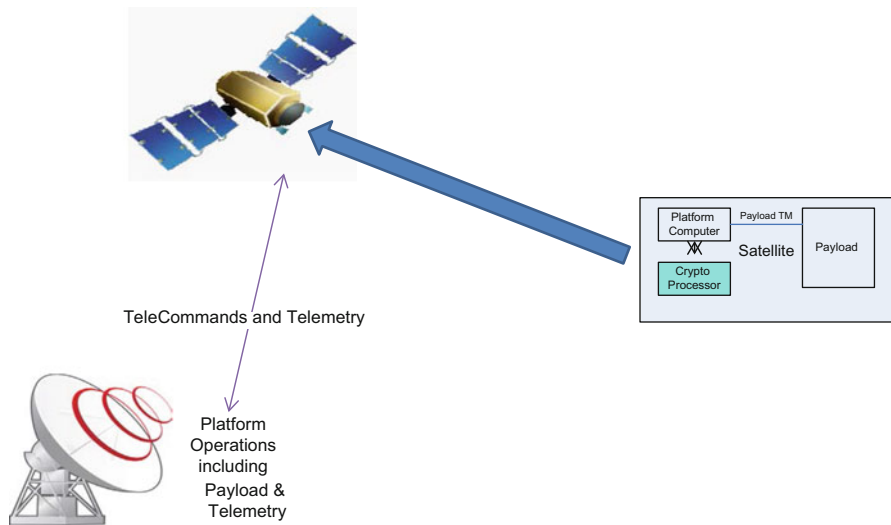
*Housekeeping telemetry* (anti-replay): Sequencing based on the introduction of a sequence number generated by a counter on board.

### Payload Data

At virtual channel level, use Advanced Encryption Standard (AES) algorithms in cipher feedback mode (CFB), output feedback mode (OFB), or in counter mode of operations (CTR), the latter recommended by CCSDS.

As far as the key management is concerned, it is necessary to be able to change the keys after a certain amount of data had been sent, to avoid the possibility of the intruder to accumulate large amounts of encrypted data and to exercise cryptanalysis on them. This can be done with *over the air rekeying* techniques (OTAR), based on preloaded master keys.

In any case, in order to be able to apply the abovementioned security measures on the ground-to-orbit link, it is fundamental that a set of cryptographic functionalities is installed on board, implemented in bespoke hardware that normally goes simply under the term “Crypto-chip,” before the launch (Fig. 4). This function is able to perform on the tele-commands and on the telemetry all the functions necessary to implement the information assurance properties, as required by the mission designers on the basis of the risk assessment specific to that mission (see next section).



**Fig. 4** Crypto-equipment on board

In addition, some missions may require that also the payload should be protected (mainly for reasons of the property of confidentiality). This implies the encryption of the whole payload, with the consequent need to renew the keys used for the encryption on a periodic basis, determined by the amount of the data to be transmitted. The same equipment can be used to that end, with the use of appropriate encryption primitives (via an application programming interface, API) to be invoked by the on-board software on each data package or on the whole data stream, to achieve the required level of protection.

---

## **ESA's Own Approach to Mission Security**

In order to address specifically the security risks for space missions that concern specifically the missions designed and operated by ESA, the ESA security office held a workshop with participation from ESA mission planners from different directorates and member states' delegations. The methodology suggested by the ISO 27005 standard (Information Technology – Security Techniques – Information Security Risk Management 2018) was applied, in order to perform the assessment and develop appropriate recommendations. The ISO 27001 is the main driver of the whole exercise on ESA systems and missions aimed at analyzing the risks and establishing an information security management system (Information Technology – Security Techniques – Information Security Management Systems – Requirements 2013).

The following recommendations stood out among those presented:

- Increase a risk awareness culture throughout the agency, by identifying the key people with the directorates and programs involved
- Mitigation of risks by improving the detection and reaction process
- Mitigation of risks coming from the supply chain when building a satellite or a ground station
- Need to create synergies between different directorates, systems, infrastructures, and actors within the agency
- Need to create a permanent security risk assessment, management, and maintenance process, based on the loop of continuous improvement (PDCA, plan-do-check-act)

It has been agreed that the goal of the exercise is to develop an “ESA policy on security risks in space programmes and mitigation measures,” to induce mission planners to address security at the moment they start their work of the definition of all the mission aspects and characteristics. At that point, the owner of the mission must decide on the mission-specific security measures, based on a risk assessment methodology, and of course must ensure the necessary funding.

The following elements stood out as elements to be included in the to-be-developed ESA policy:

- Provision of horizontal functions, building a cross-mission infrastructure providing a catalogue of basic common services to all missions, e.g., crypto-chips including standardized primitives to invoke the respective functions, software components, key management, etc.
- Selection of mission-specific functions, to be decided on the basis of the risk assessment by the mission planner, depending on types of missions, categories, and data policy (this will be developed in the following section)

In addition, the policy shall address, in a modular way:

- The different categories and the different phases of the missions (A-to-F), based on a critical assessment of the suggestions from two studies
- The cost aspects in the risk assessment model, to enable a better decision by management, proposing a way to assess and quantify the intangible costs for loss of image/reputation (reputation index)

Concerning the general aspects to be addressed, the policy shall:

- Focus on public-private partnership (PPP) for definition of missions, by involving industry in planning and support
- Ensure the involvement of small and medium enterprises (SMEs), as they increase the choice of providers, and they are often the expert in the specific fields, e. g., in software development

The policy will also have to include:

- Provisions to ensure the supply chain to avoid from any risks stemming from the use of untrusted vendors, to be applied to future missions
- A common mandatory base for all missions to address the minimum risks (loss of spacecraft, image, etc.), whereas all other specific decisions on risk mitigation shall remain with the mission owner
- Involvement of ESA mission partners including the European Defence Agency, the European Commission, Eumetsat, to be decided on a case-by-case basis.

As a complement to the policy document, as customary, at a lower level, an implementation document shall be developed, containing specific technical/commercial details and tools, to evolve over time alongside the development of technology.

Different security profiles would then have to be defined to address an increasingly stronger hierarchy of security measures, similarly to what was done by the working group on security of the Sentinels, the space components of the Copernicus program, which had defined a number of security profiles of increasing coverage and complexity and recommended to each mission the adoption of the most suitable one of them.

Secure ground-to-space connectivity is in particular being standardized at world-wide level by the CCSDS, in the data link layer security standard.



## Mission Categories and Security Profiles

There is a difference in the threats that different categories of mission can be subject to. Different mission types have actually different security requirements, based on the need to protect one or more of the five property of information assurance, plus and with priority the survival and well-being of humans (safety of life applications and manned spaceflight). Figure 5 illustrates the hierarchy of space missions based on such priorities.

The different space missions can be categorized by different categories of risks, with increasing depth and level of concerns:

- Scientific
- Earth observation
- Navigation
- Communications
- Space situational awareness
- Manned spaceflight and exploration

In order to approach the cybersecurity of missions in a systematic way leading to a streamlined engineering, corresponding to different levels of security implementation, five different protection profiles have been developed, to be applied to the different mission categories (0 to 4). They cover tele-commands, housekeeping telemetry, as well as payload data, as detailed in the following.

### **Profile 0: no specific security**

No tele-command authentication or encryption

No encryption of housekeeping telemetry or payload data

Standard terrestrial links security (firewalls, intrusion detection/prevention, security information and event management (SIEM), etc.)

Implemented, for example, in the historic ESA missions ERS/ENVISAT and the Earth Explorers, as a matter of fact, in most of the space missions until recently

### **Profile 1: static tele-command protection**

Tele-command authentication and anti-replay

Authentication key(s) preloaded on board before launch

Tele-command authentication can be enabled/disabled automatically (via a timeout mechanism) or by ground via specific protected tele-commands

Currently implemented on the ESA missions MetOp and Automated Transfer Vehicle (ATV)

### **Profile 2: dynamic tele-command protection**

Tele-command authentication and anti-replay.

Authentication keys are loaded by ground using preinstalled master keys for the encryption of the related tele-commands.

Tele-command authentication can be enabled/disabled automatically (via a timeout mechanism) or by ground via specific protected tele-commands.

Implemented in the Sentinels of the Copernicus program.

### **Profile 3: dynamic tele-command + payload data protection**

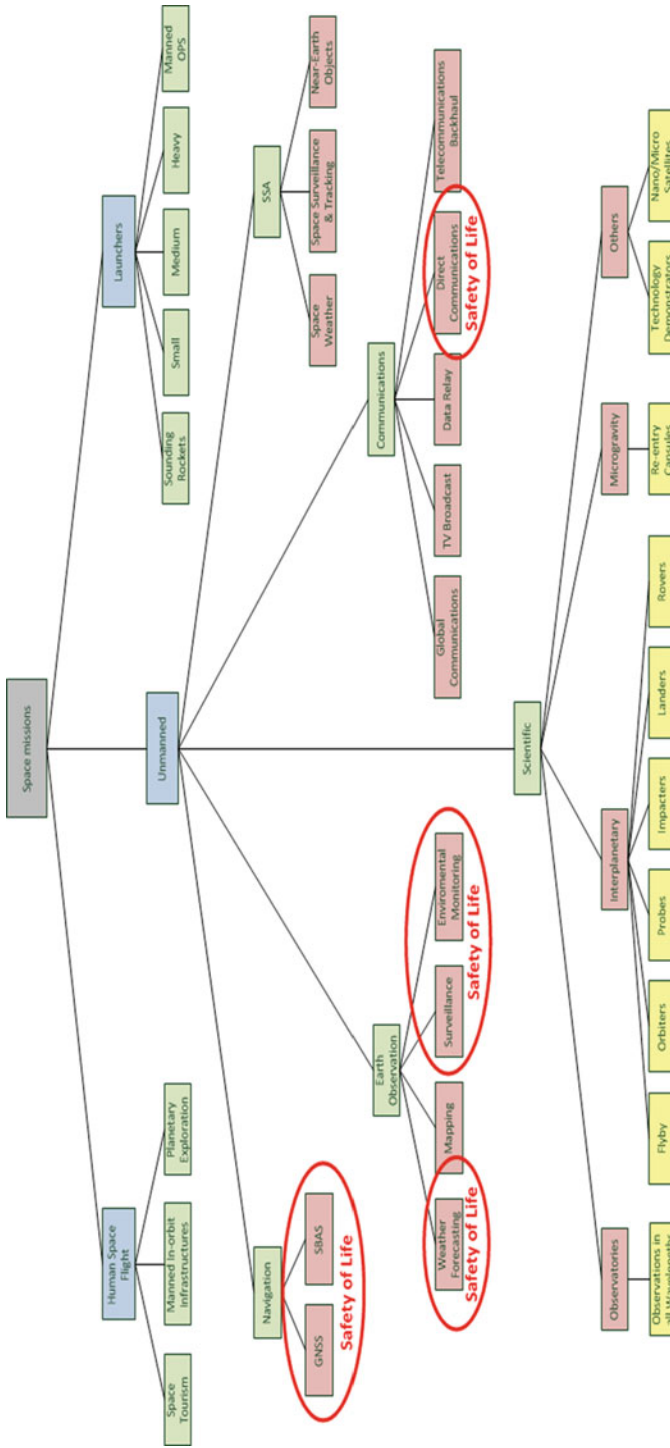


Fig. 5 Different mission categories, including those with safety of life characteristics

Payload data is also encrypted, catering to a specific data policy that requires protection and access control of the data.

Four types of keys: master keys, tele-command authentication keys, payload data encryption keys, and tele-command encryption keys.

Payload data encryption can be enabled/disabled automatically (via a timeout mechanism) or by ground via specific protected tele-commands.

**Profile 4: dynamic tele-command + payload + telemetry data protection**

Telemetry data is also encrypted.

Five types of keys: master key, tele-command authentication key, data encryption key, telemetry data encryption key, and tele-command encryption key.

Some of the data encryption can be enabled/disabled automatically (via a timeout mechanism) or by ground via specific protected tele-commands.

When a new mission is planned and designed, it is thus important that the specific threats, according to the specific mission category to streamline efforts, are analyzed and that the necessary security measures are put in place accordingly. Stitching up security upon an existing system would be, in fact, a very complex and expensive endeavor, not recommended from the managerial and financial points of view.

As a first example, we consider the Galileo program. As far as the protection of the Galileo infrastructure is concerned, the following measures are applied:

- Physical protection of the ground segment elements
- Strong interaction with host countries: critical infrastructure plan and arrangements for efficient intervention
- Location of ground stations only in EU member states, with full control of the territory

With respect to the protection of the Galileo signals in space, Profile no. 4 is selected, providing dynamic tele-command + housekeeping telemetry data protection:

- Payload protected only for particular, specifically defined services.
- End-to-end signal protection, from spacecraft to control center.
- Signal modulation features allow robustness against low-level interference, uplink diversity, and anti-jamming antennas.

As a second example, the Copernicus program has selected Scenario 2, with dynamic tele-command protection as baseline. The following security functions are performed on the Sentinel spacecraft:

- Tele-command authentication + anti-replay.
- Tele-command “encryption” limited to security-related tele-commands, like the uploading of new keys.
- “Encryption” affects *only* the tele-command “data field.”
- No housekeeping telemetry and payload data encryption.
- Preinstalled fixed master keys: used as key encryption keys.
- Session keys: used for authentication, uploaded by ground using master keys.

- Keys are referenced by meta-information avoiding the need to encrypt house-keeping telemetry.
- Tele-command authentication can be bypassed automatically upon critical mission failure.
- Tele-command authentication bypass can be enabled/disabled by ground via authenticated tele-command or by a watchdog based on timeout.

---

## Conclusions: New Space, New Cyber Threats!

It has emerged clearly in this discussion that the cybersecurity of space missions is a matter of competitiveness for the European space industry and that, at the same time, is a vital interest of the European Union that is the owner of the Copernicus and Galileo programs.

Moreover, the need to guarantee high production rates (e.g., four satellites per day in the case of the densest constellations) requires the system integrators to stretch globally the existing supply chain while including new components' providers. This introduces the additional need to ensure that the whole chain is trusted through all its components and thus subjected to strict controls (that must dive all the way down to the silicon).

The globalization of manufacturing capabilities and the increased reliance upon commodity software and hardware for space and ground segments have expanded the opportunities for malicious modification in a manner that could compromise critical functionality. This is introducing a whole family of additional risks, challenging the frontier of technology.

---

## References

- An Introduction to Computer Security—The NIST Handbook (1995) National Institute of Standards and Technology special publication 800–12. NIST, Gaithersburg, Maryland
- Anonymous Hacks The European Space Agency. <https://www.inverse.com/article/9152-anonymous-hacks-european-space-agency-releases-data-online>
- Attackers Hack European Space Agency, Leak Thousands Of Credentials 'For The Lulz'. <https://www.computerworld.com/article/3014539/attackers-hack-european-space-agency-leak-thousands-of-credentials-for-the-lulz.html>
- CCSDS Cryptographic Algorithms (2014) Informational report (green book), CCSDS 350.9-G-1, Issue 1. CCSDS, Washington, DC
- Del Monte L, Zatti S (2015) Preliminary reflections about the establishment of a cyber-security policy for a sustainable, secure and safe space environment. In: IAC-15,D5,4,3,x27636, 66th international Astronautical congress, Jerusalem, pp 12–16
- <https://en.wikipedia.org/wiki/rosat>
- <https://www.dailymail.co.uk/news/article-2055311/hackers-infiltrate-us-satellites-taken-complete-control-achieving-steps-required-command-satellite.html>
- <https://www.extremetech.com/extreme/287284-hacking-satellites-is-probably-easier-than-you-think>

- Information Security Glossary of Terms (2012) Report concerning space data system standards (green book), CCSDS 350.8-G-1, Issue 1. CCSDS, Washington, DC
- Information Technology—Security Techniques—Information Security Management Systems—Requirements (2013) International standard, ISO/IEC 27001:2013, 2nd edn. ISO, Geneva
- Information Technology—Security Techniques—Information Security Risk Management (2018) International standard, ISO/IEC 27005:2018, 3rd edn. ISO, Geneva
- Satellite Services And Interference-The Current Situation., <https://www.itu.int/en/ITU-R/space/workshops/2013-interference-geneva/presentations/Yasir%20Hassan-%20Arabsat.pdf>
- Security Threats against Space Missions (2015) Report concerning space data system standards (green book), CCSDS 350.1-G-2, Issue 2. CCSDS, Washington DC



Joe Pelton, Tommaso Sgobba, and Maite Trujillo

## Contents

Introduction .....	266
The Many Facets of Space Safety .....	268
Acceptable Safety Level .....	269
Safety Standards and Compliance Verification .....	270
Launch Safety .....	271
Launch Site Ground Safety Risk .....	271
Launch Flight Safety Risk .....	272
Launch Risk for Maritime and Air Transportation .....	274
Air-Launch Safety .....	274
On-Orbit Safety .....	276
Orbital Debris .....	276
Collision Risk with Orbital Debris .....	277
Controlling Orbital Debris Risk .....	279
Orbital Debris Remediation: Active Debris Removal .....	280
Reentry Safety Risk .....	282
Environmental Risk .....	283
Risk for Aviation .....	285
Existing Regulations and Standards .....	286

---

J. Pelton (✉)

International Association for the Advancement of Space Safety (IAASS), Arlington, VA, USA  
e-mail: [joepelton@verizon.net](mailto:joepelton@verizon.net)

T. Sgobba

International Association for the Advancement of Space Safety (IAASS), Noordwijk,  
The Netherlands  
e-mail: [tommaso.sgobba@esa.int](mailto:tommaso.sgobba@esa.int)

M. Trujillo

European Space Agency (ESA) – European Space Research and Technology Centre (ESTEC),  
Noordwijk, The Netherlands  
e-mail: [trujillo\\_m@hotmail.com](mailto:trujillo_m@hotmail.com); [maite.trujillo@esa.int](mailto:maite.trujillo@esa.int)

Human Spaceflight Safety .....	287
System Safety .....	287
Commercial Suborbital Regulatory Safety Framework: A Case Study .....	288
Human Rating: A Historical Perspective .....	292
Human Spaceflight Safety Risks .....	294
Conclusions .....	297
References .....	297

---

## Abstract

Space safety is necessary for the sustainable development and performance of space missions. Space safety best practices are important in almost any kind of space mission, manned or unmanned, commercial, scientific, exploratory, and even military. Space safety aims to protect human lives relevant infrastructures in space and on ground, and affected Earth, orbital, and planetary environments. As the pace of space exploration and commercial exploitation increases, without improved space safety practices and standards, billions of dollars (US) of space assets, many astronaut lives, and even people here on Earth could all be increasingly in peril.

This chapter introduces the many facets of safety that must be addressed by spacefaring nations around the world. This chapter assesses a wide range of space safety risks in relation to the various flight phases, from launch, to on-orbit operations, to reentry while stressing the importance of new forms of international agreement to coordinate areas such as space traffic management.

---

## Introduction

Space safety includes the protection of human life, the safeguard of critical and/or high-value space systems and infrastructures, as well as the protection of Earth, orbital, and planetary environments.

Space safety is necessary for the sustainable development of space activities. Space safety actually covers many diverse areas that are discussed in this chapter. Space safety can be defined as freedom from or mitigation of human or natural harmful conditions. These conditions can cause death, injury, illness, damage to or loss of systems, facilities, equipment or property, or damage to the environment. The term “safety” refers to threats that are nonvoluntary in nature (design errors, malfunctions, human errors, natural hazards, etc.), while “security” refers to threats which are voluntary (i.e., of aggressive nature such as use of anti-satellite weapons). In some languages, a single term is used for both, which may sometimes lead to confusion. Space safety thus covers many different areas as shown in Fig. 1. This figure shows the various fields of space safety, the relevant interest scope (national, international, or global), and the preferred processes used for risks mitigation, risk-based design, and operational hazard controls, although a mixture of the two is generally used.



**Fig. 1** Space safety fields – Credit: IAASS (International Association for the Advancement of Space Safety)

Space safety can refer to human crew and passengers, personnel directly involved in system integration and operation, personnel not directly involved but co-located, as well as the general public – whether on land, the oceans, or aloft. In the case of unmanned systems such as robotic satellites or high altitude platforms, etc., space safety refers also to (non-malicious) external causes that lead to degradation or loss of mission objectives. For example, it could include such matters as the collision between two operational satellites, or the collision of an operational satellite with space debris.

Absolute freedom from harmful conditions (i.e., safety) is impossible to achieve. To be absolutely safe, a system, product, device, material, or environment should never cause or have the potential to cause an accident. In the realization and operation of systems, the term safety is generally used to mean acceptable, or mitigated, risk levels, not absolute safety. The increasing level of activities in the stratosphere, subspace, or what is sometimes called the proto-zone (i.e., 21–160 km), is an area that will increasingly be considered as an area of concern under space safety as well.

Acceptable risk level is not the same as personal acceptance of risk, but it refers to risk acceptability by stakeholders’ community or by society in a broad sense. Acceptable risk levels vary from system to system and evolve with the passing of time due to socioeconomic changes and technological advancement. Implementing proven best practices at status-of-art is a prerequisite for achieving an acceptable risk level, or in other words to make a system “safe” or “safer.” Safety best-practices are usually established by government regulations



and norms, or by industrial standards, and enforced through authoritative organizations (e.g., government bodies or delegated independent organizations). Without enforced regulations, norms, or standards, the term safety (i.e., acceptable risk) becomes meaningless. In other words, compliance with regulations, norms, and standards represents the safety yardstick of a system.

Firstly, the chapter introduces the many facets of safety and discusses acceptable safety levels. Then, we address the risks inherent to each flight phase, from launch to on-orbit and reentry safety risks. Finally, human spaceflight safety considerations are described.

---

## The Many Facets of Space Safety

A total of 23 astronauts and cosmonauts have lost their lives since the beginning of human spaceflight. The count includes four casualties on ground during training and the most recent casualty during flight test on the part of Michael Alsbury. Alsbury died on October 32, 2014, in the crash of the suborbital Virgin Galactic SpaceShipTwo “Enterprise.” The first casualty on ground was the soviet cosmonaut trainee Valentin Bondarenko who died in a pressure chamber fire during training in March 1961. Few years later, three American astronauts were killed by a fire during training inside an Apollo capsule. There have been in total three accidents during reentry: Soyuz 1 in April 1967, Soyuz 11 in June 1971, and Shuttle Columbia in February 2003. In the latter case, in addition to the loss of crew, the public on ground and the passengers travelling by air were subjected to an unprecedented level of risk due to the US continental-wide path of falling debris, with a projected 1% chance that a fatal collision with aircraft would occur (Helton-Ingram et al. 2005).

Although a rare occurrence, space accidents are not perceived by the public simply as caused by random or unfortunate circumstances, but as the dramatic demonstration that human spaceflight programs and the entire organizations behind them failed their core mission. The risk of loss of life in human spaceflight is currently around 1 in 100 flights! Enormous, if we compare with accident rates in commercial aviation which is around 1 in 10 million flights in the USA. Although high in percentage, the loss of life in human spaceflight is still very low in absolute terms due to the low number of flights per year. Nevertheless, the entire human spaceflight program is putted in question following an accident. The reason is that the ultimate purpose of the program is the achievement of safe (and routine) physical human access to space. An accident makes clear to the public (and to political representatives) that such objective is far from being achieved. Furthermore, there is no sign of convinced effort by the cost-conscious emerging commercial human spaceflight industry in learning the lessons from 60 years of government program. They seem to prefer pursuing the development of obsolete rule-based consensus standards based on future data instead of modern techniques of risk-based design based on proven performance requirements.

Improving the safety culture of the companies, building robust safety organizations, and promoting safety education and research is paramount to maintain and expand public support for human spaceflight.

Space safety is not only about astronaut safety. Unmanned space access has become increasingly important to the great majority of countries worldwide. Upon achieving the status of a spacefaring nation, however, a key responsibility that devolves is to establish the technology and processes to protect (national and foreign) life and property against the consequences of malfunctioning rockets and reentry space systems (e.g., satellites, rockets upper stages). Safety risk in space missions also includes general public safety (on ground, on air, and at sea) and safety of launch site personnel. Space safety in a wider sense also encompasses the safeguarding of strategic and costly systems on orbit (i.e., satellites, international space station, and global utilities), valuable facilities on ground (e.g., launch pads), as well as the protection of the orbital space and of the Earth environment.

### **Acceptable Safety Level**

The safety level achieved by a system can be objectively determined by data; however, defining an acceptable level of safety is not a simple job. The definition of acceptable safety level is based not only on technical state-of-the-art considerations but also on a number of nontechnical factors such as cultural, economic, market, or political assessments. For such reason, the safety acceptability level in any field, from drinkable water to toys or nuclear power plants, is generally established by national regulations. They may differ from country to country and also evolves with time and public expectation. When international commerce is involved, such rules need necessarily to be harmonized. An example are the international safety standards for air navigation issued by the International Civil Aviation Organization (ICAO), which represent one of the most clear-cut successes in the field of international safety cooperation.

Due to the fact that there is nothing as “absolute safety” and given that the “acceptable risk” is usually a critical balance of industrial interests and public rights, the lack of national or international regulations as currently the case in the USA for the commercial human spaceflight industry represents a business survival risk, beyond the legal protection afforded by the “informed consent” approach. This is to say that without a government-defined safety standard (i.e., acceptable level of safety), an operator would have a hard time defending the vehicle actual risk level after an accident. Indeed following a fatal accident, it seems likely that the operator’s fleet would be grounded and perhaps made obsolete by newly issued (and likely strict) standards in the emotional wake of the accident. We can say that obtaining a certification of compliance with safety regulations serves the interests of the customer but at the same time also protect industry from (unbounded) tort liability by implicitly or explicitly defining the acceptable risk level at the current state of art.

For instance, in 2008, the US Supreme Court ruled in favor of a manufacturer of a balloon catheter that burst and severely injured a patient during an angioplasty. The Court wrote that the Food and Drug Administration (FDA) spent an average of 1,200 h reviewing each device application and granted approval only if found there was a “reasonable assurance” of its “safety and effectiveness.” The manufacturer argued that the device design and manufacturing had been in accordance with FDA’s regulations and that FDA and not the courts was the right forum on imposing requirements on cutting edge medical devices, arguing that “nothing is perfectly safe.”

## Safety Standards and Compliance Verification

In the safety field, it is an axiom that safety rules and compliance verification are under a single authority. There is no industry in which this principle is not applied. Usually such single authority is vested into a dedicated government organization (e.g., the Federal Aviation Administration (FAA) in the USA or the European Aviation Safety Agency (EASA) in Europe). The rapid advancement of technologies, however, pose a problem of staying abreast of technical advances. Government agencies have difficulty in keeping up with the pace of accelerating technical and scientific knowledge. One concept that is taking hold is the establishing of intermediate organizations, funded and supported by industry, i.e., so-called safety institutes, which are being tasked to develop and maintain safety standards and to verify compliance. However, care must be exercised to prevent that under the pressure of economic interests, such “self-controlling” safety-standards processes become ineffective or unduly influenced by industry interests.

The Presidential Commission that investigated the Deep Horizon oil drilling platform disaster in the Gulf of Mexico in 2011 clearly made the point about what a safety Institute should be, and how to ensure that it can effectively contribute to the continuous improvement of safety for the benefit of industry and society. The Commission identified in particular three elements: (1) commitment of companies CEOs; (2) involvement and cooperation among the best technical experts from industry (on the basis of the principle that “safety is not proprietary”); and (3) distancing these Institutes from industrial advocacy/lobbyist organizations. In this respect, the Commission noted that an organization that works as the industry’s principal lobbyist and public policy advocate cannot serve as a reliable standard-setter, because it would regularly resist anything that could make industry operations potentially more costly. Such organization would fail to reflect “best industry practices” and would express instead the “*lowest common denominator*.” “*In other words, a standard that almost all operators could readily achieve.*”

As we will see later, the risks related to space activities (e.g., launch and reentry) are often of international nature; however, currently there are no international regulations but only few national regulations, which are often scattered among different government agencies and organizations or not applied in a uniform manner

by key players. To explore the different facets of space safety, the next sections will discuss the safety risks associated to the different flight phases, from launch to on-orbit safety (e.g., space debris-related hazards) and reentry. Then, the risks inherent to human spaceflight will be introduced, both for orbital and suborbital flights.

---

## **Launch Safety**

### **Launch Site Ground Safety Risk**

On August 22, 2003, at 13:30 h (local time), a massive explosion destroyed a Brazilian Space Agency VLS-1 rocket as it stood on its launch pad at the Alcantara Launching Center in northern Brazil. Twenty-one technicians close to the launch pad died when one of the rocket's four first-stage motors ignited accidentally. The investigation report established that an electrical flaw triggered one of the four solid fuel motors while it was undergoing final launch preparations. The report said that certain decisions made by managers long before the accident occurred led to a breakdown in safety procedures, routine maintenance, and training. In particular, the investigation committee observed a lack of formal, detailed risk management procedures, especially in the conduct of operations involving preparations for launch. As of today, there have been nearly 200 people killed on ground by rocket explosions during processing, launch preparations, and launch. In the last 10 years, there have been also at least six launches which have been terminated by explosion commanded by the launch range safety officer to prevent risk for the public. There have been also several more cases of launchers that did not make to orbit, exploded on the pad, or came back prematurely to Earth in an uncontrolled fashion.

The main ground hazards during launch are explosive, toxic, or radioactive hazards. Explosive hazards (overpressure and fragments thrown by an explosion) are an important component in the launch area. Toxic hazards from the rocket's exhaust products and meteorological conditions are often an additional consideration in defining so-called exclusion areas. Additional sections of the launch complex may be restricted to protect against the kinetic energy of inert debris (i.e., spent stages) or radiation from radars and other support instrumentation. During preparation for launch, a very common issue that the ground processing safety community encounters is lack of recognition of the need for detailed ground safety documentation and rigorous technical safety reviews. Many hardware and mission designers assume that if the hardware is safe to fly, it will also be safe during ground processing. Some also assume that the industrial safety processes used during development and manufacture are sufficient for use at the launch and landing sites.

When an exclusion area is defined, each country has its own procedures for communicating the boundaries of the area. On land, this is commonly through sign postings and guards. Formal notices are frequently used to communicate with operators of ships and aircraft. Moreover, the degree of compliance varies

with location and time. When the exclusion area is near the launch complex, ranges frequently employ different forms of surveillance to determine whether any vessels have intruded into the hazardous area. When intruders can be identified, the ranges may request them to depart, passively wait for their departure, or proceed with the launch, based on the decision that the risk to the vessel is sufficiently small.

Nowadays, international commercial spaceports are proliferating, and the growing need is felt to equally and uniformly protect worldwide the local personnel as well as the foreign teams which participate to launch campaigns. When in October 2002 a Russian Soyuz exploded at launch killing a young Russian soldier who was watching the launch from the first floor of a building, it was by pure luck that no one was injured of the large international support team on site which was watching the launch from a closer location.

### **Launch Flight Safety Risk**

Knowledge of best practices and techniques in launch safety and risk assessment are not widespread and may vary greatly from country to country. Furthermore, currently during launch, a country may take risks on the population of a foreign country that even if equal to that for their own population is a unilateral decision and not the outcome of consultation. Space treaties define liabilities, but they neither define nor require uniform risk assessment and management methods and standards.

The way of achieving public protection from launch activities is by isolating the hazardous condition from populations at risk. When this is not feasible, launch vehicle performance and health is monitored for automatic or manual flight termination. Flight termination strategies are meant to limit rocket excursions from planned trajectory. The residual risk is evaluated with reference to where people may be at risk because of debris generated by flight termination.

Identification of high-hazard areas may range from simplistic rules of thumb to sophisticated analyses. When simple rules are applied, they commonly specify a hazard radius about a launch point and planned impact points for stages, connected by some simple corridor. More sophisticated analyses attempt to identify credible rocket malfunctions, model the resulting trajectories, and determine the conditions that will result in debris such as exceeding the structural capacity of the rocket or a flight termination action by a range safety officer. These analyses typically include failure analyses to identify how a launch vehicle will respond under various failure scenarios. This will include failure response analyses to define the types of malfunction trajectories the vehicle will fly. The vehicle loads are assessed along the malfunction trajectory to determine whether structural limits will be exceeded. Vehicle position and velocity may be compared against abort criteria to assess whether the vehicle should be allowed to continue flight, terminate thrust, or be destroyed. Debris-generating events then become the basis for assessing the flux of debris falling through the atmosphere and the impact probability densities. The debris involved may be screened by size, impact kinetic energy, or other criteria to assess which fragments pose a threat to unsheltered people, people

inside various types of buildings, people on ships, and people in aircraft. The resulting debris impact zones are then commonly used as part of the basis for defining exclusion areas.

Although full hazard containment is considered to be the preferred protection policy, it is not always possible. The next line of protection after defining exclusion areas is real-time tracking and control of the rockets. Range safety systems are used for this purpose. They include a means of tracking a launch vehicle's position and velocity (tracking system) and a means of terminating the flight of a malfunctioning vehicle (flight termination system).

Flight termination criteria are customarily designed based on the capability of the range safety system to limit the risk from a malfunctioning launch vehicle. Frequently, ranges assume that they can reliably detect a malfunctioning launch vehicle and terminate its flight whenever good quality tracking data is available. This assumption is based on high-reliability designs customarily used for range safety systems. At present, however, there are no international design standards for range safety systems. Moreover, efforts to assure that the design standard does, in fact, achieve the intended reliability levels are rare.

The final tiers of protection are risk analysis and risk management. Residual risks from the launch are quantified and assessed to determine if they are acceptable. This step involves an extension of the model outlined above for assessing hazardous areas. It is common to perform these protection steps in an iterative manner, using the results of each step to adjust the approach to the others until the desired level of safety is achieved with acceptable impacts on the proposed launch. The current practice is to assess risks for each launch and to approve the launch only when risk levels are acceptable. Unlike most other activities, annual risk levels are addressed by exception.

A proper risk analysis addresses the credible risks from all launch-related hazards. These may include inert debris, firebrands, overpressure from exploding fragments, and toxic substances generated by normal combustion as well as toxic releases from malfunctions. When assessing launch risks, as it occurs for reentry, it is important to account for all exposed populations: people on land, people in boats, and people in aircrafts. Proper consideration must be given to the effect of sheltering (i.e., type of construction and materials of houses, buildings) on the risks. It is often assumed that neglecting sheltering will overstate the risk. When sheltering is adequate to preclude fragment penetration, this assumption is valid. When fragments are capable of penetrating a structure, debris from the structure increases the threat to its occupants. As launch vehicles proceed downrange, they typically leave the territorial domain of the launching country and begin to overfly international waters and the territory of other countries.

Tolerable risks for a launch are commonly expressed in terms of a collective or societal risk level and risk to the maximally exposed individual (individual risk). Collective risk is commonly expressed as the number of individuals statistically expected to be exposed to a specified injury level. Individual risk is commonly expressed as the probability that the maximally exposed individual will suffer the specified injury level. The two most commonly used levels of injury are fatality

and serious injury. When it is difficult to quantify risk directly, impact probability for specified classes of debris is often used as a proxy measure. Thus, for example, it is customary to protect people on ships or people on airplanes by creating exclusion zones based on impact probabilities.

Outside of the immediate launch area, surveillance is more difficult and more costly. Consequently, most ranges use surveillance very selectively outside of the immediate launch area, typically restricting surveillance to planned impact areas for spent stages and other planned jettisons. As a result, publishing exclusion areas at these distances is much less effective. More efficient tools for surveying these remote locations and communicating with intruders would enhance the effectiveness of protecting ships and aircraft in these areas.

## **Launch Risk for Maritime and Air Transportation**

Controlling risks to seafaring vessels from space launch activities is most successful when mariners are notified about hazard areas and when the responsible launching agency surveys the potentially affected areas to detect intruders and to warn them to leave the exclusion area. Following a mishap, communication with these vessels to proceed at maximum speed in a prescribed direction to minimize impact probability is essential to control undue risks. Currently, costs and technology limit surveillance and communication to locations near land.

For launch preparations, the management of airspace must also consider aircraft traffic. At present, there are limited capabilities for addressing this issue. The Federal Aviation Administration (FAA) has begun an initiative to address these concerns for US operations. It should be noted that the current practice is for each launch range to manage risks on a mission-by-mission basis through Launch Collision Avoidance (LCOLA) processes. Minimal attention is paid to annual risks generated by the range's launch operations. There is no agency – national or international – that monitors and controls risk posed to overflown populations. A city may be placed at risk by launches from multiple launch sites without the performance by involved launching nations of any coordinated assessment to assure that the risk levels are acceptable.

Citizens of all countries should be equally protected from the risk posed from overflying by launch vehicles and returning spacecraft(s). The common practice is to make these determinations on a launch-by-launch basis with no consideration of previous, planned, or future launches.

## **Air-Launch Safety**

Launching from ground means that the first stage of the rocket will be traveling through the denser layers of the atmosphere where drag is a significant issue. The launchpad is at a fixed location, selected to meet logistics, safety, and

environmental constraints, not always the most favorable one to reach orbit. What if one could do away with the first stage and replace it with a high-altitude platform, such as an aircraft or a balloon? Compared with ground launch, air-launch provides flexible and reusable “first stage” and a lighter expendable rocket.

To place a satellite on low Earth orbit, let us say at 300 km, you need to reach a velocity of about 9.4 km/s. Because the starting velocity is zero, we can also talk of it as difference of velocity, or delta-V, of 9.4 km/s. The delta-V depends on several parameters, like initial altitude, speed, and angle of attack. If we launch, for example, from a balloon at 15 km, with zero launch velocity and 0° angle of attack, the required delta-V is 8.8 km/s. If we launch from an aircraft flying at 1,200 km/h, the delta-V drops to 8.5 km/s. It further drops to 8.3 km/s if the launch angle of attack is 30°. Delta-V reductions translate into lighter rocket, less fuel, and lower cost.

On 13 June 1990, Pegasus of Orbital Sciences Corporation became the first commercial air-launch vehicle. Released from a modified Lockheed L-1011 airliner, Pegasus can put a satellite of 450 kg in low Earth orbit.

In the past, the market of small satellites (100–500 kg) and miniature satellites, which comprises microsattellites (10–100 kg) and nanosatellites (1–10 kg), was small. They were usually launched as secondary payloads on larger launch vehicles. Nowadays, the commercial and military market of small and miniature satellites is the fastest growing segment of the space launch business, and several companies are developing air-launch vehicles specifically targeted to such market. Ability to “launch on demand” at low cost will allow launch operators to offer unprecedented flexibility for schedule and orbital placement. Several air-launch systems are under development as adaptation of commercial and military airplanes or as dedicated systems. Any country or operator with experience of military supersonic aircraft has the potential to develop its homegrown micro- and nanosatellites air-launch service.

In July 2012, Virgin Galactic announced that their rocket called LauncherOne would be air-launched from the same WhiteKnightTwo aircraft carrier they developed for suborbital human spaceflight. Later a Boeing 747, called Cosmic Girl, has been adapted for the purpose. Air-launch operations will start in 2019.

Stratolaunch Systems is developing a gigantic new air-launch system. The project comprises three main components: the carrier aircraft being built by Scaled Composites, a multistage rocket, and a mating and integration system. Stratolaunch’s carrier aircraft has wingspan of 117 m and a weight of over 540,000 kg including the fully fueled launch vehicle. The test flights of the carrier aircraft are planned in 2019.

The diffusion worldwide of air-launches raises the issue of safety. The record of current spacefaring countries in performing traditional ground-based launches is not uniform. It may seriously worsen for air-launches because of lack of experience of newcomers. Most of what we know about air-launch safety comes from Orbital ATK Pegasus and from supersonic air-launches performed by USAF and NASA. As of 2018, Orbital ATK Pegasus was launched 44 times safely, but in two cases the rocket veered off course and was destroyed by command sent by range officer.



Orbital ATK Pegasus launches are performed under safety oversight of one of the US launch ranges. Some key points:

- (a) Rocket assembly and payload integration processes are identical to those followed for traditional expendable rockets. Safety rules are identical.
- (b) Integration of rocket on aircraft carrier is performed on an isolate runway section, subjected to safety rules similar to pad operations. Safety requirements for barriers to prevent inadvertent rocket ignition are identical with those for ground launches, but arming is done in flight close to launch time.
- (c) Aircraft flight to reach the launch location is subjected to constraints. For example, it is forbidden to overfly populated areas.
- (d) Launch is performed following a countdown process with teams and equipment on-board the aircraft carrier and remotely at the range.
- (e) Rocket flight is redundantly tracked. Manual commands are sent for flight termination, if it leaves the planned trajectory (use of mobile range equipment). Special procedures are defined for the case of launch abort.
- (f) Air traffic is cleared in advanced from launch location, but procedures are not tightly enforceable, as for launches from ground. In the latter case, the spaceport and the airspace overhead can be “sealed.” For air-launches, which usually take place from the international airspace therefore outside national authority, only advisory NOTAMs can be sent to alert the air traffic.

---

## **On-Orbit Safety**

### **Orbital Debris**

Space is not an empty vacuum but contains both natural debris (i.e., micrometeoroids, interplanetary dust) and human-made space debris. Humans generally have no involvement in natural debris; thus, here we will concentrate exclusively on human-made debris. Orbital debris generally refers to any human-made material on orbit which is no longer serving its intended function. There are many sources of debris. One source is discarded hardware such as upper stages of launch vehicles or satellites which have been abandoned at the end of their operational life. Another source is spacecraft items released in the course of mission operations. Typically, these items include launch vehicle fairings, separation bolts, clamp bands, adapter shrouds, and lens caps. Various shapes and sizes of debris are also produced as a result of the degradation of hardware due to atomic oxygen, solar heating, and solar radiation and also from combustion of solid rocket motors. Examples of such products are paint flakes, aluminum oxide exhaust particles, and solid motor-liner residuals.

Fifty years of spaceflight have cluttered the space around the Earth with an enormous quantity of human-made debris. Scientists assume that there are approximately 500,000 objects in orbit whose sizes are above 1 cm. Currently, about 22,000 of such objects (i.e., 10 cm in diameter or larger) are being tracked by the US Space Surveillance Network (including about 1,000 objects representing

functional satellites). The number is expected to rise significantly as new large-scale satellite constellations are deployed in the future to provide communications, remote sensing, and other services such as frequency monitoring.

When the new S-band radar “Space Fence” is fully operational, this number will increase to a much larger number and will be able to track objects down to the size of a marble in Low Earth Orbit (LEO). Among the tracked pieces of debris, there are about 200 satellites abandoned in Geostationary Earth Orbits (GEO) occupying or drifting through valuable orbital positions and posing a collision hazard for functional spacecraft(s). The survival time of the debris can be very long. Objects in 1,000 km orbits can exist for hundreds of years. At 1,500 km, the lifetime can go up to thousands of years. Objects in geosynchronous orbit can presumably survive for one million years.

The future population of orbital debris will depend upon whether the creation or removal rate dominates. Currently, the only mechanism for removal of debris is orbital decay through atmospheric drag, which ultimately leads to atmospheric reentry. This mechanism is only effective in a restricted range of low Earth orbits (LEO). At higher orbits, it takes hundreds to thousands of years for objects to reenter the Earth’s atmosphere. Consequently, there is no effective removal mechanism. Historically, the creation rate of debris has outpaced the removal rate, leading to a net growth in the debris population in low Earth orbit at an average rate of approximately 5% per year. A major contributor to the current debris population has been fragment generation via explosions. As the debris mitigation measure of passivation (e.g., depletion of residual fuel) comes to be implemented more commonly, it is expected that explosions will decrease in frequency. It may take a few decades for the practice to become implemented widely enough to reduce the explosion rate, which currently stands at about four per year.

Several environment projection studies conducted in recent years indicate that, with various assumed future launch rates, the debris populations at some altitudes in LEO will become unstable. Collisions will take over as the dominant debris generation mechanism, and the debris generated will feed back into the environment and induce more collisions. The most active orbital region is between the altitudes of 900 and 1,000 km, and even without any new launches, this region is highly unstable (Liou and Johnson 2006). It is projected that the debris population (i.e., objects 10 cm and larger) in this “red zone” will approximately triple in the next 200 years, leading to an increase in collision probability among objects in this region by a factor of ten. In reality, the future debris environment is likely to be worse than was suggested, as satellites continue to be launched into space.

## **Collision Risk with Orbital Debris**

Orbital debris generally moves at very high speeds relative to operational satellites. In LEO (i.e., altitudes lower than 2,000 km), the average relative impact velocity is 10 km/s (36,000 km/h). In the geostationary orbits, the relative velocity is lower, approximately 2 km/s, because most objects move in an eastward direction orbit.

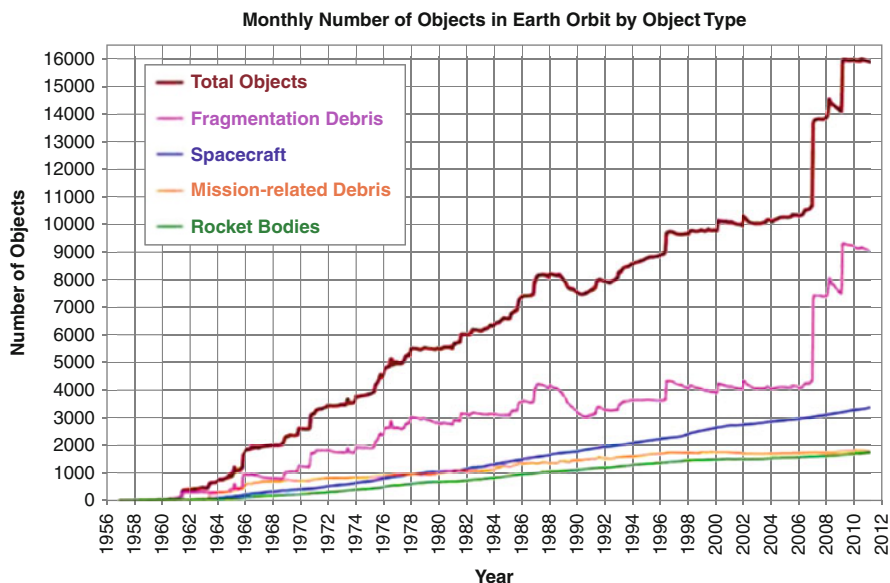
At these hypervelocities, pieces of debris have a tremendous amount of kinetic energy. A 1 kg object at a speed of 10 km/s has the same amount of kinetic energy that a fully loaded truck, weighing 35,000 kg, has at 190 km/h. A 1-cm-sized aluminum sphere at orbital speed has the energy equivalent of an exploding hand grenade. A 10 cm fragment in geosynchronous orbit has roughly the same damage potential as a 1 cm fragment in low Earth orbit.

Pieces or particles of debris smaller than 1 mm in size do not generally pose a hazard to spacecraft functionality. Debris fragments from 1 mm to 1 cm in size may or may not penetrate a spacecraft, depending on the material composition of the debris and whether or not shielding is used by the spacecraft. Penetration through a critical component, such as the flight computer or propellant tank, can result in loss of the spacecraft. NASA considers pieces of debris 3 mm in size and above as potentially lethal to the retired Space Shuttle and the International Space Station. Debris fragments between 1 and 10 cm in size will penetrate and damage most spacecraft. If the spacecraft is impacted, satellite function will be terminated, and at the same time, a significant amount of small debris will be created. If a 10 cm debris fragment weighing 1 kg collides with a typical 1,200 kg spacecraft, over one million fragments ranging in size from about 1 mm and larger could be created. Such collisions result in the formation of a debris cloud which poses a magnified impact risk to any other spacecraft in the orbital vicinity (e.g., other members of a constellation of satellites).

Certain regions of the debris cloud are constricted to one or two dimensions. Such constrictions do not move with the debris cloud around its orbit. They remain fixed in inertial space while the debris cloud repeatedly circulates through them. In many satellite constellations, there are multiple satellites in each orbital ring. If one of these satellites breaks up, the remaining satellites in the ring will all repeatedly fly through the constrictions. If many fragments are produced by the breakup, the risk of damaging another satellite in the ring may be significant. If satellites from two orbital rings collide, two debris clouds will be formed with one in each ring. The constrictions of each cloud will then pose a hazard to the remaining satellites in both rings.

In February 2009, a nonoperational Russian satellite, Cosmos 2251, collided with Iridium 33, a US commercial telecommunication satellite, over Siberia at an altitude of 790 km. This collision, the first of its kind, was the worst space debris event since China intentionally destroyed one of its aging weather satellites during an antisatellite missile (ASAT) test, in 2007. The Iridium satellite that was lost in the collision was part of a constellation of 66 low Earth-orbiting satellites providing mobile voice and data communications services globally. As expected, the risk of collision of other Iridium satellites in the same plane dramatically increased with daily announcements of possible collisions (i.e., conjunctions) with Iridium 33 debris. Fig. 2 presents the evolution in time of the number of human-made debris objects, which highlights the increasing problem impacting the sustainability of the space environment.

In general, orbital debris collision is among the top risk for human spaceflight. The 2003 Shuttle risk assessment performed after the Columbia accident, the first



*Monthly Number of Cataloged Objects in Earth Orbit by Object Type: This chart displays a summary of all objects in Earth orbit officially cataloged by the U.S. Space Surveillance Network. "Fragmentation debris" includes satellite breakup debris and anomalous event debris, while "mission-related debris" includes all objects dispensed, separated, or released as part of the planned mission.*

**Fig. 2** Catalogued human-made space objects in Earth's orbit (Credit: NASA)

one that incorporated the threat posed by orbital debris, determined that the likelihood of orbital debris bringing down the Shuttle was far greater than that of the widely feared failures of main engines, solid rocket boosters, or thermal protection. Orbital debris colliding with different spots of the wing flaps was the most likely catastrophic failure. Damage would have rendered the wing flap (elevon), unable to steer and slow the Shuttle during the reentry phase.

Orbital debris collision is the primary source of risk for the International Space Station (ISS). To minimize such risk for the crew, the ISS is shielded. The ISS is indeed the most heavily shielded spacecraft ever flown. All together there are 100 different shields protecting the ISS. Critical components such as habitable compartments and high-pressure tanks will be able to withstand the impact of debris as large as 1 cm in diameter.

## Controlling Orbital Debris Risk

Orbital debris risk is best controlled by limiting creation through a number of design and operational measures, like "passivation," collision avoidance maneuvers, and end-of-life disposal.

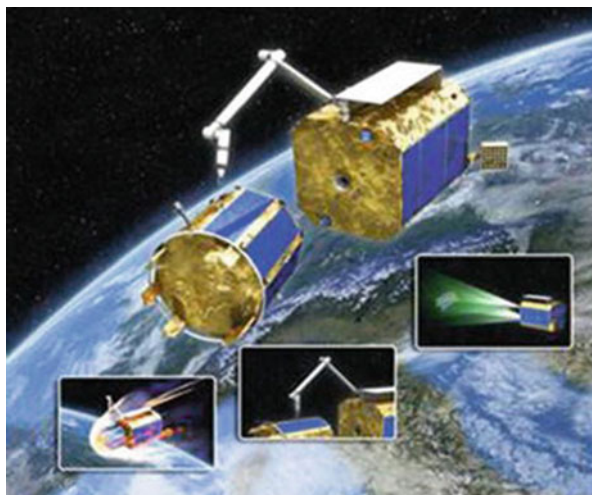
Passivation is the term used to describe the prevention of satellite and upper-stages explosions by controlled removal of stored energy at the end of useful life. For example, propellant in upper stages and satellites can be eliminated by either venting or burning to depletion. This process is applied primarily to low earth orbit satellites. Batteries can be also designed to reduce risk of explosion.

Spacecraft maneuvers, when possible, can also mitigate orbital debris risk of collision. The International Space Station has maneuvered on several occasions to avoid collisions with orbital debris. Also, in the case of satellite constellations, because a potential collision will lead to the creation of a debris cloud that may result in damage to other members of the constellation, collision avoidance maneuvers may be necessary. Another means to reduce the risk of collision is to remove satellites and upper stages from mission orbits, the so-called protected orbits, at the end of operational life. Currently, UN guidelines and other internationally agreed standards (e.g., ISO 24113) recommend that a space system should not remain in its mission orbit for more than 25 years. Such objective is met either by lowering the orbit such that residual atmospheric drag is sufficiently strong to cause decay and reentry or by moving the spacecraft to a “graveyard orbit” outside of protected regions. At orbits above 2,000 km, it is not economically feasible to force reentry within 25 years. Spacecraft operating in the geosynchronous orbits are routinely boosted into a higher disposal orbit at the end of their mission life, except in case of malfunction. Propellants need to be reserved to perform the disposal maneuvers. There are penalties in the form of reduced performance and/or mission life linked to the disposal of space systems. Estimates of the amount of “lost” lifetime for geosynchronous satellites vary between 6 months and 2 years. For example, it has been calculated that if a typical commercial communication satellite that has 24 Ku-band and 24 C-band transponders with bandwidths of 36 MHz has to be boosted into a higher disposal orbit at the end of its mission life, this maneuver would cause the satellite operator an average loss (in terms of how much longer the satellite could have continued commercial operations) of as much as 1 year’s profit. This problem can be mitigated by employing the so-called inclined orbit operation so as to preserve fuel since North–South station-keeping requires more than ten times more fuel than East–West station-keeping.

### **Orbital Debris Remediation: Active Debris Removal**

In view of the massive amount of debris already in existence in Earth orbits, growing consensus among experts suggests that an active process for the removal of existing debris from space is required, as mitigation is no longer sufficient to ensure the long-term sustainability of outer space activities. Active debris removal (ADR), specifically the removal of nonfunctional spacecraft and spent upper stages, requires the development of advanced technologies and concepts (Fig. 3). Their implementation also raises a number of difficult technical, economic, strategic, institutional, legal, and regulatory challenges that must be addressed at the very outset. For such on-orbit services to become available, the following elements need

**Fig. 3** Active debris removal concept (Credit: DRL)



to be in place: service at the lowest possible cost, spacefaring countries committing to gradually remove their own debris, and new national licensing regulations mandating removal (autonomous or enforced) at the end of mission.

To achieve the lowest possible service costs, international technological cooperation, high rate of missions per year, and possibly multiple service targets per mission would be needed at least for an initial period of operations. The international technological cooperation would serve the purpose of making available all existing technologies and share the cost of new developments. Servicing with a single flexible system multiple (international) customers and perform multiple removals within the same mission would also substantially contribute to lower the operational costs. To a certain extent, the same path used once for the development of the satellite telecommunication industry may be repeated with the establishment of an intergovernmental organization on the model of the early International Telecommunications Satellite Organization (INTELSAT) which would later evolve into full commercial services. Another alternative would be to create an international fund for debris removal. Such a fund could start as national and/or regional cooperative and evolve into an international fund supported by all spacefaring nations. The problem with all such plans or concepts is that the current provisions of Article VII of the Outer Space Treaty of 1967 as well as those of the so-called Liability Convention of 1972 structure “liabilities” associated with such removal activities in such a way as to give little incentives for countries to actively remove debris from orbit.

The development of new technological capabilities, in the area of active debris removal and possible repurposing of the defunct spacecraft, continues apace. There have been a series of projects sponsored by the U.S. Defense Advanced Research Projects Agency (DARPA), by NASA, by DLR of Germany, and by private companies such as McDonnell Detwiler, Vivasat, and Conesat. On June 20, 2018, the “Remove Debris” proof of concept small satellite was launched

through the Kaber Launch facility operated by Nanoracks from the International Space Station. This small satellite with a mass of only 100 kg will be able to test a range of possible removal techniques. It was constructed by Surrey Space Technology Ltd. and after some 5 years of development is now testing these removal strategies. (“NanoRacks Deploys Largest Satellite from International Space Station to Date,” July 2, 2018. <https://mail.aol.com/webmail-std/en-us/suite>).

---

## Reentry Safety Risk

As previously mentioned, nonfunctional satellites, spent launch vehicle upper stages, and other orbital debris do not remain in low Earth orbits indefinitely but gradually return to Earth due to residual atmosphere drag. In low Earth orbits, natural orbital decay can take place within few months or requires hundreds or even thousands of years to happen depending on the altitude.

As nonfunctional satellites, spent launch vehicle stages, and other pieces of debris enter denser regions of the atmosphere, they fragment and sometimes explode due to high aerodynamic forces combined with loss of materials strength due to heat caused by friction with air at high velocity. Heat would subsequently cause the demise of major portions of the hardware due to melting and vaporization. However, between 10% and 40% of the original mass will survive and reach Earth’s surface. In general, parts and components made of aluminum and similar materials with low melting temperatures do not survive reentry, while those made of materials with high melting temperatures, such as stainless steel, titanium, do survive. Also parts with low mass and large surface area, and therefore large aerodynamic drag, will survive due to slow down and related low heating. The surviving fragments represent a hazard to people and property on the ground. They also represent a potential serious risk to air and maritime traffic.

Due to variability of the atmosphere layers around the Earth, it is difficult to predict the exact reentry time of a randomly reentering satellite or upper stage. As a consequence, it is very difficult to predict where surviving fragments will hit the surface of the Earth. Over the last 50 years, more than 1,400 metric tons of materials are believed to have survived reentries. The largest object to reenter was the Russian Mir Space Station, which weighed 120,000 kg. Reentries are frequent, in particular upper-stages reentries. In 2011, launch vehicles upper stages reentered at a rate of 1 per week with a total mass that was five times that of uncontrolled spacecraft reentries for the same period (Figs. 4 and 5). Many of the reentered parts recovered on ground, including tanks up to 250 kg weight, belonged to rockets.

Currently, a number of countries prescribe that the risk of any personal casualty due to a single reentry event must be less than 1 in 10,000 reentries. France has the most conservative requirement of less than 2 in 100,000 reentries. Of particular concern, although very remote, is the risk for aviation and the emotional and psychological impact on the general public that a single accident with many casualties would cause (Ailor and Wilde 2008), as described in section “[Risk for Aviation](#).”

**Fig. 4** Stainless steel propellant tank of second-stage Delta 2 reentered launch vehicle (US, 1977) (NASA courtesy)



**Fig. 5** Reentered titanium motor casting of third-stage Delta 2 (Saudi Arabia, 2001) (NASA courtesy)



## Environmental Risk

There is health risk related to launch ascent failures and reentry of space systems (e.g., rocket bodies and nonfunctional space systems). During normal launches, stages separate sequentially and fall down to Earth. Most launch trajectories and spaceport locations are chosen to ensure that the impact areas are outside populated areas and mainly contiguous to the oceans. Nevertheless, there are inland spaceport locations and land overflying trajectories which lead to stages dropping to ground in sparsely inhabited areas with ensuing soil contamination. Approximately 9% of the propellant from a launch stage remains in the tank once it is dropped. The penetration of contaminants depends on the nature and properties of the soil and can lead to the contamination of groundwater as well as surface water. For example, hydrazine (UDMH) is often used in hypergolic rocket fuels as a bipropellant in



combination with the oxidizer nitrogen tetroxide and less frequently with IRFNA (red-fuming nitric acid) or liquid oxygen. UDMH is a toxic carcinogen and can explode in the presence of oxidizers. It can also be absorbed through the skin. A tablespoon of hydrazine in a swimming pool would kill anyone who drank the water. In a study conducted by Vector, the Russian State Research Center of Virology and Biotechnology in Novosibirsk, health records from 1998 to 2000 of about 1,000 children in two areas in southern Siberia polluted due to launches from Baikonur spaceport in Kazakhstan were examined, comparing them with 330 records from a nearby unpolluted control area. Grouping all cases of disease together, the research team concluded that children from the worst-affected area were up to twice as likely to require medical attention for diseases such as endocrine and blood disorders during the 3 years studied and needed to be treated for twice as long. Contamination can be far worse and massive in case of launch failure. In September 2007, the explosion of a Russian Proton M rocket contaminated a vast swath of agricultural land in Kazakhstan with 200 t of toxic fuel.

Reentries may also cause concern because of the toxicity or radioactivity of materials on board. On 21 February 2008, an uncontrolled reentering satellite was shot down on grounds of public safety. The satellite was destroyed at an altitude of 247 km by a ship-launched missile. The malfunctioning spacecraft, a US spy satellite (USA 193), carried 450 kg of highly toxic frozen hydrazine fuel in its titanium fuel tank. In addition, it was expected that about 50% of the satellite's mass of 2,270 kg would survive reentry, thus adding to public risk on ground.

Currently, there are 32 defunct nuclear reactors circling the Earth as well as 13 reactor fuel cores and at least 8 radio-thermal generators (RTGs). RTGs had been used six times in space missions in low Earth orbits up to 1972 and twice in the geostationary geosynchronous orbit up to 1976. Since 1969, another 14 reactors have been used on lunar and interplanetary missions. The total mass of RTG nuclear fuel in Earth orbit today is in the order of 150 kg. Another form of nuclear power source used in space activities is a nuclear reactor. Most of these reactors were deployed on Soviet radar reconnaissance satellites (RORSATs) launched between 1965 and 1988.

Among the space nuclear accidents (i.e., unwanted/unplanned release of radioactive material), two involved orbital debris, and a third was a close call. In 1978, the RORSAT COSMOS 954 failed to separate its nuclear reactor core and to boost it into a disposal orbit as planned. The reactor remained on board the satellite in an orbit that decayed until it reentered the Earth's atmosphere. The satellite crashed near the Great Slave Lake in Canada's Northwest Territories, spreading its radioactive fuel over an area of about 124,000 km<sup>2</sup>. Recovery teams swept the area by foot for months. Ultimately, they were able only to recover 12 large pieces which comprised a mere 1% of the estimated quantity of radioactive fuel on board. These pieces emitted radioactivity of up to 1.1 Sv/h. (It should be noted that usually a nuclear emergency is declared on ground at 500  $\mu$ Sv/h.) A few years later, in 1982, another RORSAT, COSMOS 1402, failed to boost the nuclear reactor core into a storage orbit. The ground controller managed to separate the core from the reactor itself to make it more likely that it would burn up in the

atmosphere before reaching the ground. The reactor was the last piece of the satellite to return to Earth in February 1983 when its core fell into the South Atlantic Ocean.

Then, in April 1988, yet another Russian spacecraft, COSMOS 1900, failed again to separate and boost the reactor core into a storage orbit. However, later on, the redundant system succeeded in separating and boosting the nuclear core into a storage orbit, although lower than that originally planned.

## **Risk for Aviation**

Many of the practices that apply to launch apply also to reentry, but the latter pose special issues because they are mainly random or related to unique behavior of the reusable vehicle during reentry.

The disintegration during reentry of the Shuttle Columbia on February 1, 2003, was a watershed moment in the history of launch and reentry safety analysis. It highlighted the need to select vehicle reentry trajectories which minimize the risk to ground populations and the need to take measures to keep air traffic away from falling debris if a reentry accident occurs. The Columbia accident initiated a chain of events that demonstrated the need for a deliberate, integrated, and, eventually, international approach to public safety during launch and reentry operations. This is especially true for the management of air traffic and space operations.

Shortly after the breakup of Columbia over a relatively sparsely populated area of Texas, dramatic images of the debris from the breakup were seen around the globe: an intact spherical tank in a school parking lot, an obliterated office rooftop, mangled metal along roadsides, and charred chunks of material in fields. The NASA Administrator testified before the US Senate that it was “amazing that there were no other collateral damage” (i.e., that no members of the public were hurt).

The Columbia Accident Investigation Board (CAIB) raised and answered many questions relevant to public safety during launch and in particular reentry. Given the available data on the debris recovered and the population characteristics in the vicinity, a CAIB study found that the absence of ground casualties was, in fact, the statistically expected result. Specifically, based on census data and modeling methods consistent with US standards and requirements set by other US agencies (e.g., the USAF in the Air Force Space Command Manual and by the FAA in the Federal Register), the study found that “the lack of casualties was the expected event, but there was a reasonable probability (less than 0.5 but greater than 0.05) that casualties could have occurred.” However, a similar event over a densely populated area such as Houston would almost certainly have produced multiple casualties among the public on the ground.

At the time of the Columbia accident, NASA had no formal policy regarding public risk during Shuttle reentry. Following the CAIB report, NASA established a new safety policy (NPR8715.5). The NASA public safety policy embraced many

of the risk measures and thresholds already in use by other US agencies, such as individual and collective risk limits in terms of casualties. However, NASA's public safety policy also putted forward innovative criteria for risk budgets governing distinct phases of flight which have gained broad acceptance. Therefore, the Columbia accident led to greater consensus and innovation in the management of risk to people on the ground from launch and reentry operations.

The Columbia accident also promoted the development of improved methods and standards for aircraft safety during launch and reentry. Following the release of the final report of the CAIB, the FAA funded a more detailed aircraft risk analysis that used the actual records of aircraft activity at the time of the accident. That study found that the probability of an impact between Columbia debris and commercial aircraft in the vicinity was at least one in a thousand, and the chance of an impact with a general aviation aircraft was at least one in a hundred. The analysis used the current models which assume that any impact anywhere on a commercial transport with debris of mass above 300 g produces a catastrophic accident: all people on board are killed. Current best practices are captured in RCC 321-07 "Common Risk Criteria for the National Ranges," which provides a vulnerability model for the commercial transport class. In 2008, the FAA and USAF sponsored the development of vulnerability models for transoceanic business jets based on the same methods.

After the release of the CAIB report, the FAA investigated the need for new decision support tools to better manage the interface of space and air traffic. The relevant procedures were then developed, and they are currently in use as a real-time tactical tool in the event of a catastrophic event like the Columbia accident to identify how to redirect aircraft around a space vehicle debris hazard area.

---

## Existing Regulations and Standards

The sections above have provided an overview of risks associated to launch, on-orbit operations, and reentry. As it has been illustrated, the issues raised above involve risks that are national and/or international in nature. For launch and reentry activities, national regulations exist in some spacefaring nations; however, no international regulation applicable worldwide has been agreed. There have been ever-increasing safety concerns that are now posed by the pollution of the orbital environment (i.e., orbital debris) to operational spacecraft and the international space station. After many years of debate, international space debris mitigation guidelines have been worked out by the Inter-Agency Space Debris Coordination Committee (IADC), and these have been agreed as voluntary standards within the umbrella of the United Nations Committee of Peaceful Usages of Outer Space Activities (UN COPUOS). In addition, the International Organization for Standardization (ISO) has published a standard on space debris mitigation (i.e., ISO 24113) to put forward design and

operational practices for implementation in future space systems to minimize the generation of orbital debris.

However, no remediation activities are yet internationally agreed, and therefore, neither standards nor regulations exist in this field. In addition, although different countries have the observational assets to perform space situational awareness services, currently, there are no agreed space traffic management regulations. Clearly these two issues, i.e., space debris mitigation and space traffic management, will constitute the two most important international space safety standards and regulatory issues to be faced in the next few years.

---

## Human Spaceflight Safety

In the following sections, the risks associated to human spaceflight will be presented. Firstly, the concept of system safety for crewed systems would be introduced. Then, the value of regulations and safety standards would be illustrated by real examples in different fields, and a case study based on the emerging industry of commercial suborbital transportation will be examined. Then, the historical and latest developments for human-rating space systems would be presented, and finally, a selected number of risks associated to human spaceflight will be covered.

## System Safety

Prior to the 1940s, flight safety consisted basically of trial and error. The term fly-fix-fly was associated with the approach of building a prototype aircraft, fly it, and repair/modify if broke, and fly it again. For complex and critical systems, such approach is simply impossible. From 1952 to 1966, the US Air Force (USAF) lost 7,715 aircraft in noncombat operations, in which 8,547 persons were killed. As reported by Olsen (2010), “most accidents were blamed on pilots, but many engineers argued that safety had to be designed into aircraft just as any other functional or physical feature related to performance. Seminars were conducted by the Flight Safety Foundation, headed by Jerome Lederer that brought together engineering, operations, and management personnel. At one of those seminars, in 1954, the term ‘system safety’ was first used in a paper by the aviation safety pioneer C.O. Miller.”

In the 1950s, when the Atlas and Titan ICBMs were being initially developed, there was no safety program. Within 18 months after the fleet of 71 Atlas F missiles became operational, 4 blew up in their silos during operational testing. The worst accident occurred in Searcy, Arkansas, on August 9, 1965, when a fire in a Titan II silo killed 53. The US Air Force then developed system safety assessment and management concepts. Such efforts eventually resulted into the establishment of a major standard, MIL-STD-882D, and System Safety Engineering as a discipline (Leveson 2003).

## Commercial Suborbital Regulatory Safety Framework: A Case Study

One of the areas of space safety regulation that has received the most attention in recent years has been with regard to overseeing the safety of commercial spaceflights – particularly in the form of suborbital flights.

A suborbital flight is defined as a flight up to a very high altitude beyond 100 km above sea level but in which the vehicle involved does not go into orbit (i.e., does not attain an orbital speed exceeding 11.2 km/s). A suborbital trajectory is defined under US law as “The intentional flight path of a launch vehicle, re-entry vehicle, or any portion thereof, whose vacuum instantaneous impact point does not leave the surface of the Earth.” Unmanned suborbital flights have been common since the very beginning of the space age. Sounding rockets covering a wide range of apogees even well above the altitude of the Shuttle and ISS orbits have been routinely launched. Nowadays, suborbital human spaceflight is gaining popularity as demonstrated by the increased interest in space tourism. Still in its nascent phase, the space tourism industry proposes new commercial vehicles which have configurations and operational mode very similar to some early government programs, namely, capsules (e.g., Mercury Redstone) or winged-rocket system (e.g., X-15 aircraft). It should be noted that the two configurations drive very different safety requirements. Safety requirements for the launcher/capsule configuration have been in place for more than 40 years and have been successfully proven, mainly during the performance of (more challenging) orbital flights. The safety requirements for the aircraft-type configuration have a well-established technological basis in the aeronautical engineering field, although they are not reflected in any current civil aviation-type regulation. The experimental aircraft X-15 flew 199 times flights before program cancellation in 1968. The X-15 suffered four major accidents (Fig. 6).

In 2004 and then in 2011, the USA passed the so-called Commercial Launch Amendments Act (CSLAA) and the “Commercial Space Launch Activities” Act that was signed into law in January 2012.

Most recently, the USA enacted H.R.2262 – U.S. Commercial Space Launch Competitiveness Act which has become Public Law No: 114-90 (11/25/2015). This law has four parts that include Title I (Spurring Private Aerospace Competitiveness and Entrepreneurship), Title II (Commercial Remote Sensing), Title III (Office of Space Commerce), and Title IV (Space Resource Exploration and Utilization). This new legislation has a variety of shorter term and longer term space safety implications and oversight and licensing arrangements for commercial space launches for manned and unmanned flights. (H.R.2262 – U.S. Commercial Space Launch Competitiveness Act).

The issuance of the new Space Policy Directive-3 in August 2018 that assigned to the new Office of Commercial Space the responsibilities of addressing for commercial space activities both responsibilities for improved space situational awareness and addressing space traffic management issues will the U.S. Department of Defense will address these issues for security and strategic purposes creates a new



**Fig. 6** X-15 crash (Credit: NASA)

path forward for the USA. This Directive set for the problem and the way forward to achieve greater space safety in the following manner.

“The future space operating environment will also be shaped by a significant increase in the volume and diversity of commercial activity in space. Emerging commercial ventures such as satellite servicing, debris removal, in-space manufacturing, and tourism, as well as new technologies enabling small satellites and very large constellations of satellites, are increasingly outpacing efforts to develop and implement government policies and processes to address these new activities.”

“To maintain U.S. leadership in space, we must develop a new approach to space traffic management (STM) that addresses current and future operational risks. This new approach must set priorities for space situational awareness (SSA) and STM innovation in science and technology (S&T), incorporate national security considerations, encourage growth of the U.S. commercial space sector, establish an updated STM architecture, and promote space safety standards and best practices across the international community.”

“The United States recognizes that spaceflight safety is a global challenge and will continue to encourage safe and responsible behavior in space while emphasizing the need for international transparency and STM data sharing. Through this national policy for STM and other national space strategies and policies, the United States will enhance safety and ensure continued leadership, preeminence, and freedom of action in space.” (Space Policy Directive-3, National Space Traffic Management Policy, June 18, 2018. <https://www.whitehouse.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/>).

It was suggested at the European Space Policy Institute Autumnal Conference in September 2018 that it might be possible for spacefaring nations to undertake a parallel approach to improved space situational awareness and space traffic

management as outline in the U.S. Space Policy Directive-3 so that common and coordinated approach to these critical areas of space safety might be undertaken. The proposal made suggested the following: “U.S. Space directive 3 sets new U.S. objectives for ‘space situational awareness’, the need for an improved registry of space objects in Earth orbit, the need for better sharing of information with regard to operational spacecraft and space debris, the need for an improved space traffic management system and support for collision avoidance services.” If other spacefaring nations were to do the same, then a cooperative framework to cooperate in all these areas might be agreed. This could lead to improved security of space operations or space infrastructure security. (Joseph N. Pelton A Path Forward to Improved Space Security: Better Information Sharing, Space Situational Awareness, Space Traffic Management, and More” European Space Policy Institute Autumn Conference, Sept 28, 2018, Vienna, Austria)

The IAASS (International Association for the Advancement of Space Safety) has been particularly concerned with the safety of commercial space systems carrying passengers into space and has developed a safety certification standard that has now been published by the SAE as of July 2018. This standard addresses responsibilities, implementation, and mission safety risk. (SAE International to Publish New IAASS Standard for Commercial Space Travel and Exploration 2018-08-06 WARRENDALE, Pa. August 2018. <https://www.sae.org/news/press-room/2018/08/sae-international-to-publish-new-iaass-standard-for-commercial-space-travel-and-exploration>)

### **Self-Regulations: Safety as Business Case**

An alternative to government regulations is self-regulations. They are essentially meant to promote a higher level of safety as a business case. Take the example of Formula 1 car racing. In the first three decades of the Formula 1 World Championship, inaugurated in 1950, a racing driver’s life expectancy could often be measured in fewer than two seasons. It was accepted that total risk was something that went with the badge. It was the Imola Grand Prix of 1994 with the deaths of Roland Ratzenberger and Ayrton Senna (as shown on direct broadcast TV) that forced the car racing industry to look seriously at safety or risk to be banned forever. In the days after the Imola crashes, the FIA (Fédération Internationale de l’Automobile) established the safety Advisory Expert Group to identify innovative technologies to improve car and circuit safety and mandated their implementation and certification testing. Nowadays, Formula 1 car racing is a very safe multibillion dollar business of sponsorships and global television rights, an entertainment for families that can be enjoyed without risking shocking sights.

Another example comes from the oil industry. The Presidential Commission that investigated the “Deepwater Horizon” disaster in the Gulf of Mexico in April 2010 (11 workers killed plus an oil spill that caused an environmental catastrophe) recommended the establishment of an independent safety agency within the Department of the Interior and that “the gas and oil industry must move towards developing a notion of safety as a collective responsibility. Industry should establish a ‘Safety Institute’ [ . . . ] this would be an-industry created, self-policing entity aimed

at developing, adopting, and enforcing standards of excellence to ensure continuous improvement in safety and operational integrity offshore.”

Nowadays, sophisticated techniques are available to remove or control hazards in new systems such to minimize the safety risk of new systems before they enter into operation. Such techniques go generally under the name of “safety case.”

### **Prescriptive Requirements Versus Safety Case**

The RMS Titanic struck an iceberg on her maiden voyage from Southampton, England, to New York and sank in the early hours of 15 April 1912. A total of 1,517 people died in the disaster because there were not enough lifeboats available. During the Titanic construction, Alexander Carlisle, one of the managing directors of the shipyard that built it, had suggested using a new type of larger davit, which could handle more boats giving Titanic the potential of carrying 48 lifeboats providing more than enough seats for everybody on board. But in a cost-cutting exercise, the customer (White Star Line) decided that only 20 would be carried aboard thus providing lifeboat capacity for only about 50% of the passengers (Titanic 1912). This may seem as a carefree way to treat passengers and crew on board, but as a matter of fact, the Board of Trade regulations stated that all British vessels over 10,000 t had to carry 16 lifeboats. Obviously, the regulations were out of date in an era which had seen the size of ships reaching the 46,000 t of the Titanic.

The above accident illustrates at the same time what is a prescriptive requirement (i.e., an explicitly required design solution for an implicit safety goal) and how it can sometimes dramatically fail. Instead the safety case regime is based on the principle that the regulatory authority sets the broad safety criteria and goals to be attained while the system developer proposes the most appropriate technical requirements, design solutions, and verification methods for their fulfillment. In other words, the safety case regime recognizes that it is the regulatory authority’s role and responsibility to define where the limit lies between “safe” and “unsafe” design (i.e., the safety policy in a technical sense), but it is the developer/operator that has the greatest in-depth knowledge of the system design and operations.

A safety case is documented in the Safety Case Report that typically includes the following: (a) the summary description of the system and relevant environment and operations; (b) identified hazards and risks, their level of seriousness, and applicable regulatory criteria/requirements; (c) identified causes of hazards and risks; (d) description of how causes (of hazards and risks) are controlled; and (e) description of relevant verification plans, procedures, and methods.

The safety of the entire International Space Station (ISS) program is based on a process of incremental safety reviews by independent panels of safety case reports (called safety data packages) prepared by systems developers/operators in response to the (generic) safety requirements (NASA SSP 30599 2009). In the course of the operations, further submittals are made to account for configuration changes, previously unforeseen operations, and corrective actions from on-orbit anomalies.



## Human Rating: A Historical Perspective

Since the first space programs that achieved human access to space, the identification of system requirements for crewed space systems has been a complex exercise. In the 1950s, the engineering efforts to maximize safety were built on the experience gained about the space environment from unmanned vehicles and experimental platforms with chimpanzees on board, which contributed to gather data for planned crew missions. The concept of human rating (also known previously as manned rated) was used to refer to systems designed to carry humans into space. However, a formal common process designated to grant human-rating certification did not exist at the time, as it is being used in current programs. In the past, the methods for implementing human rating varied as a function of program, across system and subsystems and sometimes across mission phases within a program.

In 1995, 14 years after the Shuttle had entered operations, an agency-wide committee was tasked to develop a human-rating requirements definition for launch vehicles based on conventional (historical) methods. After the revision of past programs both for launchers and spacecrafts such as Gemini, Apollo, and the Space Shuttle, the committee recommended the following definition of human-rating process, that is, “a process that satisfies the constraints of cost, schedule, performance, risk and benefit while addressing the three requirements of human safety, human performance, and human health management and care” in a document reviewing the historical perspective of human rating of US spacecraft (Zupp 1995). Historically, the human-rating process for Mercury, Gemini, and Apollo programs had been centered on human safety. The Skylab and Shuttle programs added to this an emphasis on human performance and health management. Further details on the history of these programs can be found in Logsdon and Launius (2008).

For Gemini as well as for other vehicles since then, an important part of assuring crew safety was the development of a crew escape system in case of abort scenarios. The escape system test program was also quite extensive, leading to the identification of improved designs throughout the testing phase and spanned a 3-year period, which lead to the development of a crew escape system, with an ejection seat qualified for flight crew space from pad aborts to 45,000 ft (Ray and Burns 1976). For the Apollo program, launch vehicles (i.e., Saturn IB and V) were designed for human spaceflight (given that no other launcher was able to deliver the required performance). These vehicles had additional redundancy and safety improvements as compared to its predecessors for Mercury and Gemini. Additionally, there was an extensive ground and unmanned flight plan to validate new design features and to certify the launch escape system uniquely developed for Apollo.

For the Space Shuttle, the considerations for crew safety were a tremendous challenge over previous programs mainly because with its configuration (where the Orbiter vehicle and the crew were much closer to the source of explosive yield of fire and overpressure than in the in-line series burn configurations used on the Mercury, Gemini, and Apollo launch systems). The most significant challenge was how to address the issue of abort during first stage. To enable

the possible consideration of crew escape, crew ejection, launch pad ejection, or Orbiter separation and fly way, a method for thrust termination of solid rocket boosters (SRBs) had to be developed. It was a technology that was not proven. Various concepts for thrust termination were examined (i.e., pyrotechnically blow out the head end of the booster and neutralize thrust; another concept was to sever the nozzle to accomplish the same result), but all raised major concerns or introduced significant design challenges. Therefore, a decision was made that the additional safety risks and design complexities introduced by thrust termination were of greater concern than the presumed low failure rate of solid motors. For the areas of “high” risk, more stringent design requirements were derived to build in greater reliability for Shuttle SRBs (i.e., structural design factors of safety, case insulation, and segment seals). The Shuttle used a historical performance database to improve safety design and certified the vehicle to be human rated with no first-stage abort capability. The focus was on system-level integrated methodology.

The human-rating process builds upon data and knowledge acquired during development, manufacturing, and operations. The information derived from the evaluation and analysis of this data can only contribute to strengthening the understanding of failure mechanisms and identifying mitigation strategies to address them. Taking into account the lessons learnt from past programs as well as the technological developments of our time, the need for specific requirements for human rating a space system to enhance crew safety and incorporate the knowledge gained through more than 40 years of space activities materialized with the release of the NASA NPR 8705.2A “Human-Rating Requirements and Guidelines for Space Flight Systems” in 2003. In this first standard addressing human-rating certification, NASA proposed the following definition: “a human-rated system is one that accommodates human needs, effectively utilizes human capabilities, controls hazards and manages safety risk associated with human spaceflight, and provides to the maximum extent practical, the capability to safely recover the crew from hazardous situations.”

In 2008 and then in 2011, NASA reissued and updated these requirements (i.e., NPR 8705.2B) with slight modifications from its original version, document that was later updated in 2011. This document contains a set of programmatic and technical requirements that establish a benchmark of capabilities for human-rated space systems. It directs programs to perform human error analysis, evaluate crew workload, conduct human-in-the-loop usability evaluations, prove that integrated human-system performance test results are required to validate system designs, and establish a Human System Integration team to evaluate these activities (Hobbs et al. 2008). NASA Constellation Program (i.e., Ares launchers and Orion capsule) was the first program to incorporate these new human-rating requirements. In parallel, activities are undergoing by other agencies (e.g., ESA and JAXA) for the refinement of safety technical requirements for human-rated space systems (Trujillo and Sgobba 2011). In 2011, the Commercial Crew Program (CCP) issued the CCT-1100 Series that communicates roles and responsibilities, technical management processes supporting certification, crew transportation systems, and ISS-related requirements for potential commercial providers.

## Human Spaceflight Safety Risks

The principal safety issues related to orbital human spaceflight are protection from environmental hazards whether space weather (i.e., ionizing radiation) or space debris, the need to provide escape and safe-haven capabilities, and prevention of collision risk. Collision risk may be divided into (1) the risk of collision during proximity operations (i.e., rendezvous and docking) and (2) risk of collision with other space traffic.

### Environmental Risk: Ionizing Radiation

The Earth's magnetic field traps electrically charged radiation particles in two belts high above the Earth. The highest extends out to about 40,000 km, and the lowest belt begins at about 600 km above the surface. The intensity of radiation in these belts can be more than a million times higher than on the Earth. For several decades to come, commercial orbital human spaceflight will most probably be limited to low Earth orbit flights where the radiation level is small or negligible. Based on the experience of several decades of human spaceflight in low Earth orbit (Vetter et al. 2002), a safe level of radiation exposure has been defined as that which would increase the lifetime risk of cancer by 3%, and this translates into a total dose of 100–400 rem depending on age and gender (Cucinotta et al. 2011). For comparison, a maximum of 10 rem is the annual dose allowed for workers in occupations involving radiation. Since health risk increases with the total dose, it is important to monitor the dose and to establish norms for the retirement of (commercial) astronauts who reach that level (NRC 2012).

### Space Safe and Rescue: Past, Present, and Future

The 1912 Titanic disaster, with a distress message telegraphed in Morse code, was a defining moment in starting the organization of search-and-rescue on a global scale. The shock of the disaster led to the establishment of means for constant distress surveillance on land and aboard ships. In 1914, the first International Convention for the Safety of the Life at Sea (SOLAS) made it an obligation for ships to go to the assistance of other vessels in distress. The system developed and matured gradually in the following decades, and in the early 1950s, it was extended to aviation, but it was only in 1985 that a well-organized international search-and-rescue (SAR) system came into force under the International Convention on Maritime Search and Rescue of 1979. The current international SAR system is based on close coordination between international maritime and aviation organizations and relies on uniform worldwide coverage and use of global space-based monitoring and tracking resources available on board GEO and LEO spacecraft (COSPAS-SARSAT Programme).

As with any comparable system, the safety of crew and passengers on board future suborbital and orbital commercial space vehicles will not depend only on design adequacy, robustness of construction, and the capability to tolerate failures and environmental risks but also upon special provisions which would allow escape, search, and timely rescue in case of emergencies. During a suborbital commercial

human spaceflight, an emergency may lead to search and rescue operations at sea or on land not dissimilar from those of an aviation accident. The case of an on-orbit emergency is different, and for that special cooperation, provisions and interoperable means need to be developed. Here, the closest parallel is that of submarine emergencies. Many nations now regularly practice multilateral rescue exercises and coordinate their rescue means and capabilities through the International Submarine Escape and Rescue Liaison Office (ISMERLO).

### **Ascent Emergencies**

During the ascent phase, a so-called abort scenario needs to be considered in order to safeguard the life of the crew and passengers on board a commercial space vehicle. Such scenarios apply to any type of space vehicle and would require also planning and cooperation with foreign countries.

Taking the experience of the Shuttle program as an example, depending on the time a malfunction would have occurred, there were Shuttle international launch abort sites at Halifax, Stephenville, St. Johns, Gander, and Goose Bay (all in Canada). There were also Shuttle transoceanic abort landing sites (TAL) at Ben Guerir Air Base, Morocco; Yundum International Airport, Banjul, The Gambia; Moron Air Base, Spain; Zaragoza Air Base, Spain; and Istres, France. Finally, there were 18 designated Shuttle emergency landing sites spread among Germany, Sweden, Turkey, Australia, and Polynesia, several of which are active international airports. For the purpose of providing the Shuttle program with the necessary assistance, access, and dedicated capabilities at those foreign landing sites worldwide, the US government had to negotiate a large number of specific bilateral agreements. In the future, when commercial human suborbital and orbital spaceflights become common, commercial entities will not be able to gain the same level of assistance on land or at sea and access to foreign facilities unless the necessary international civil space agreements and regulations are put in place by some sort of international space regulatory body similar to ICAO for aviation (Jakhu et al. 2010).

### **Crashworthiness**

Additionally, from the lessons learned of the Columbia accident and based on the findings of the Columbia Accident Investigation Board (CAIB), tasked by NASA to conduct a thorough review of both the technical and organizational causes of the loss of the Space Shuttle Columbia. The CAIB recommended that future vehicles should incorporate the following: (a) a design analysis for breakup to help guide design toward the most graceful degradation of the integrated vehicle system and structure to maximize crew survival; (b) crashworthy, locatable data recorders for accident/incident flight reconstruction; (c) improvements in seat restraint systems to incorporate the state-of-the art technology to minimize crew injury and maximize crew survival in off-nominal acceleration environments; and (d) advanced crew survival suites (including conformal helmets with head and neck restrain devices similar to the ones used in professional automobile racing) and avoidance of materials with low resistance to chemicals, heat, and flames among others.

## **Orbital Rescue**

In 1990, an International Spacecraft Rendezvous and Docking conference was held at the NASA Johnson Space Center. The purpose was to explore the need and international consensus to establish a set of common space systems design and operational standards which would allow docking and on-orbit interoperability in case of emergency. The attributes for such international standards were summarized as follows: (a) each party could implement them with their own systems and resources; (b) cooperation in such standards does not require subordination (i.e., one party does not have to buy parts of the system from another); (c) success of one project or project element is not required to insure success of the other; (d) no one standard requires subordination to another standard; and (e) the functional requirements of the standard can be implemented with a number of alternative technologies. Definition of the standards does not require the transfer of technology.

In 2008, the objective of developing orbital rescue capabilities was restated by the US Congress in the NASA Authorization Act of that year (H.R. 6063). In fact, Sect. 406, EXPLORATION CREW RESCUE, stated that: "In order to maximize the ability to rescue astronauts whose space vehicles have become disabled, the Administrator shall enter into discussions with the appropriate representatives of space-faring nations who have or plan to have crew transportation systems capable of orbital flight or flight beyond low Earth orbit for the purpose of agreeing on a common docking system standard."

In 2010, the international docking system standard (IDSS), based on the original androgynous docking system (APAS) developed in the seventies as part of the Apollo-Soyuz Project, became finally a reality through the initiative of the countries participating to the International Space Station program. Although China was not involved in such standardization effort, the Chinese had already chosen as docking system for their Shenzhou vehicle and for the Tiangong-1 space station a docking system variant called APAS-89, which is the same used on the International Space Station (ISS) and is compatible with the new international docking standard. The Chinese docking system was successfully demonstrated on-orbit in 2011 with a robotic mission. In 2012, further dockings were performed by two Shenzhou (9 and 10), both of with crew board. Following Tiangong 1, a more advanced space laboratory, dubbed Tiangong 2, was launched in 2013 followed by Tiangong 3 in 2015. In the coming years, at least two space stations will be orbiting Earth, the ISS and the Chinese Tiangong, thus making possible for the first time an orbital rescue system. Even private space stations are now envisioned by Bigelow Aerospace with prototypes now in orbit.

In 2004, a cooperative program was launched to implement such capability on the model of the International Submarine Escape and Rescue Liaison Office (ISMERLO) to "establish endorsed procedures as the international standard for submarine escape and rescue using consultation and consensus among submarine operating nations." As for submarines, also in space, the delay between an accident and rescue attempt must be short. Furthermore, the institutionalized contacts and

increased transparency engendered by such cooperation orbital rescue would fit with broader trends toward increasing openness and could constitute an important confidence-building mechanism for wider cooperation in making space operations safe and sustainable.

---

## Conclusions

This review has presented a wide variety of space risks. It has explored the safety risks that experienced space organizations and new spacefaring nations are facing. An in-depth understanding of these risks is important to fully comprehend the scope of the safety challenges ahead. Without such an understanding, it will be difficult if not impossible to mitigate them in an effective manner. Both unmanned orbital space systems and crewed vehicles are adversely affected by the growing amount of orbital debris. The cascading effect produced by space objects is a mounting concern. We must seek to minimize the impact of uncontrolled reentering objects that affect the safety of those on land, air, and sea. In addition, the proliferation of new commercial ventures indicates the need to promote space safety in the area of orbital and suborbital tourism and raises the question as how space traffic management might be addressed in future years. The complexity of space safety issues and the scope and nature of future safety challenges may well need to be tackled through an expanded international regulatory framework – one expanded to address the space safety risks that have been described in this chapter.

---

## References

- Ailor W, Wilde P (2008) Requirements for warning aircraft of re-entering debris. In: Proceedings of IAASS conference on space safety (2010) Huntsville, Alabama
- Cucinotta F, Kim M-HY, Chappell LJ (2011) Space radiation cancer risk projections and uncertainties – 2010. National Aeronautical and Space Administration, Washington, DC. (publisher)/TP-2011-216155
- Helton-Ingram S et al. (2005) Federal Aviation Administration report to the space and air traffic executive board on the plan to mitigate air traffic hazards posed by the space shuttle return to flight re-entry. FAA, Washington, DC. (publisher)
- Hobbs A, Adelstein B, O'hara J, Null C (2008) Three principles of human-system integration. In: Proceedings of the 8th Australian aviation psychology symposium, Melbourne
- Jakhu R, Sgobba T, Trujillo M (2010) An international civil aviation and space organization. In: Proceedings of IAASS conference, 2010, Huntsville, Alabama
- Leveson N (2003) White paper on approaches to safety engineering. MIT
- Liou LC, Johnson NL (2006) Instability of the present LEO satellite populations. COSPAR
- Logsdon M, Launius R (2008) Human spaceflight: projects Mercury, Gemini, and Apollo. NASA Smithsonian Press, Washington, DC, pp 2008–4407
- NRC – Committee for Evaluation of Space Radiation Cancer Risk Model (2012) Technical evaluation of the NASA model for cancer risk to astronauts due to space radiation. National Academies Press, Washington, DC
- Olsen JA (2010) A History of Air Warfare. Potomac Books, Washington

- Ray HA, Burns FT (1976) Development and qualification of Gemini Escape System. NASA TN D-4031
- Safety Review Process (2009) International space station program, NASA SSP 30599, Rev. E. Resource document. <http://kscsma.ksc.nasa.gov/GSRP/Document/ssp%2030599%20reve.pdf>. Accessed 1 June 2012
- “Titanic” Inquiry project. Resource Document (1912). <http://www.titanicinquiry.org/BOTInq/BOTReport/BOTRep01.php>. Accessed 1 June 2012
- Trujillo M, Sgobba T (2011) ESA human rating requirements: status. In: Proceedings of the IAASS Conference on Space Safety, Versailles
- Vetter R, Baker ES, Bartlett DT, Borak TB, Langhorst SM, McKeever SWS, Miller J (2002) Operational radiation safety program for astronauts in low-earth orbit: a basic framework, Report No. 142
- Zupp G (1995) A perspective on the human-rating process of U.S. spacecraft: both past and present. National Aeronautics and Space Administration, Washington, DC. (publisher)



# Evolution of Space Traffic and Space Traffic Management

# 16

William Ailor

## Contents

Introduction .....	300
Objects in Orbit .....	300
Protected Regions .....	300
GEO Protected Region .....	302
LEO Protected Region .....	303
Space Debris .....	304
Space Situational Awareness Services .....	306
Space Situational Awareness Data .....	306
Best Practices and Standards .....	307
Changes Coming .....	308
Large LEO Constellations .....	309
Environmental Effects on Satellite Lifetime .....	312
Reentry Disposal of Satellites from Large Constellations .....	313
Active Debris Removal (ADR) .....	314
Effect of Large Constellations on SSA Service Requirements .....	314
Space Situational Awareness and Traffic Management Service Providers .....	315
Conclusions .....	315
References .....	317

## Abstract

In 2016, the notion that the local space environment would continue to evolve at rates defined by previous satellite launch histories changed dramatically when SpaceX requested permission to place over 4400 satellites in low Earth orbits. Prior to that time, predictions were that the space environment could be stabilized by space operators abiding by rules and guidelines designed to limit the growth of debris. While all proposed satellites might not be realized, major changes in the

---

W. Ailor (✉)

Center for Orbital and Reentry Debris Studies, The Aerospace Corporation, El Segundo, CA, USA  
e-mail: [william.h.ailor@aero.org](mailto:william.h.ailor@aero.org)



near-space environment are coming and may come quickly. This chapter provides background, discusses potential changes, and highlights new polices and services that could arise.

## Introduction

### Objects in Orbit

Figure 1 shows the growth in the number of operating satellites and debris since the beginning of the space age by object type, Fig. 2 shows orbiting objects sorted by orbit class, and Fig. 3 shows the number of objects per cubic kilometer as a function of altitude.

### Protected Regions

Several years ago, spacefaring nations recognized that two regions of near-Earth space are particularly important to space-based services and set these regions aside as “protected regions.” The first is the low Earth orbit (LEO) protected region shown in Fig. 4 (Region 4). This region extends to 2000 km above the Earth’s surface and is heavily used by satellites that provide communication, Earth monitoring, and other services.

The second protected region is the ring of space surrounding Earth where satellites in geosynchronous equatorial orbits (GEO) operate (Region 3). This is

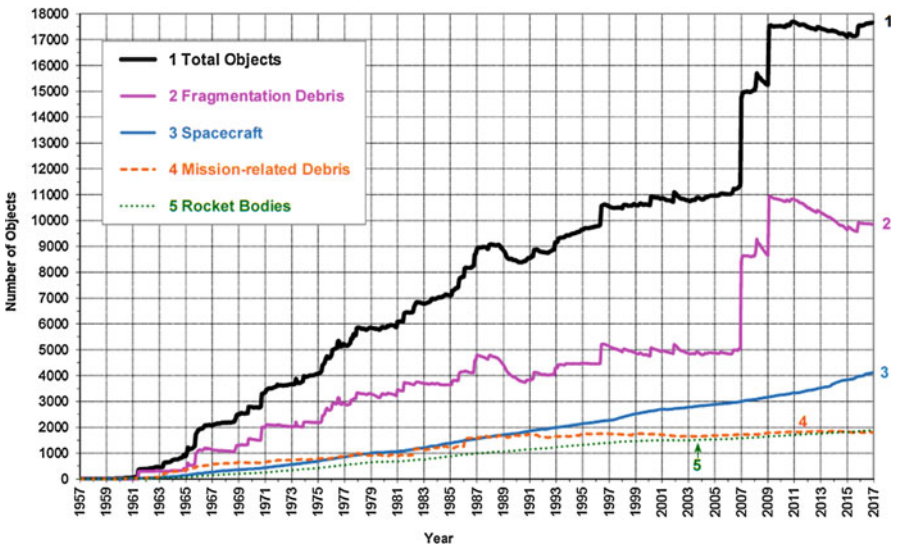
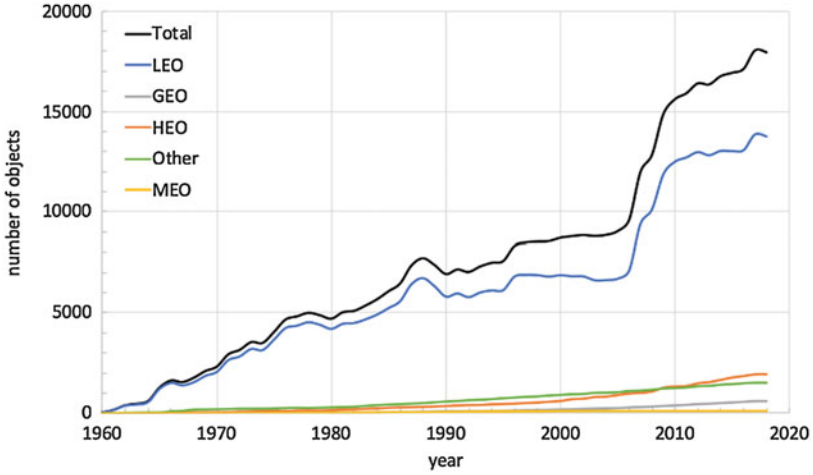
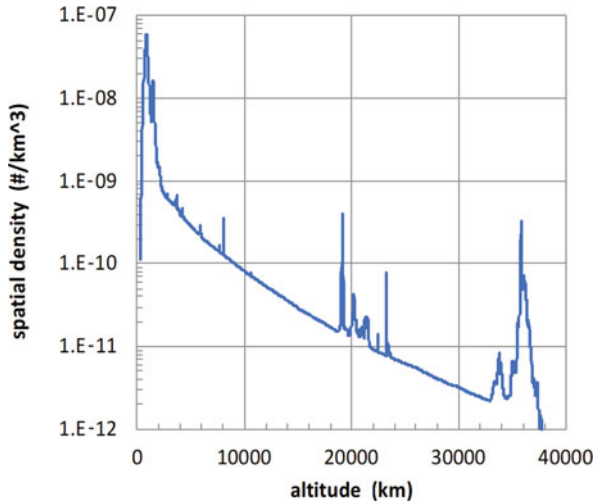


Fig. 1 Number of objects in Earth orbit by year and object type (courtesy NASA)



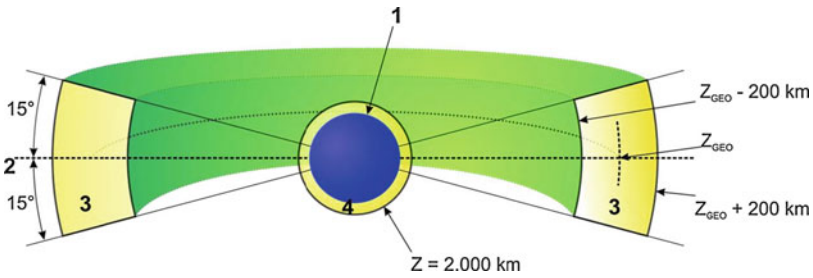
**Fig. 2** Number of objects by year and orbit class (LEO, MEO, GEO, HEO)

**Fig. 3** Number of objects/ cubic km as a function of altitude in 2018



where many large communication and weather monitoring satellites operate at fixed locations above specific regions of Earth.

A region not formally protected but should be avoided when disposing of satellites is the medium Earth orbit (MEO) region between 19,700 and 20,700 km above the Earth’s surface. This region is home to Global Positioning System (GPS), Glonass, Compass, and Galileo constellations. Due to the critical nature of the navigation and other services these constellations support, current end-of-mission satellite disposal guidelines recommend that orbits for space hardware being disposed avoid passing through this region.



**Fig. 4** Protected regions (Key: 1 Earth; 2 equatorial plane; 3 GEO protected region; 4 LEO protected region; Z altitude measured with respect to a spherical Earth whose radius is 6378 km; Z<sub>GEO</sub> altitude of the geostationary orbit with respect to a spherical Earth whose radius is 6378 km) (from ISO 24113:2019)

Highly elliptical orbits (HEOs) are orbits with high eccentricity, and vehicles in these orbits can pass through LEO, MEO, and GEO regions.

## GEO Protected Region

In addition to approximately 470 operating satellites in the GEO protected regime, there are more than 1300 tracked objects (objects larger than 1 meter) and also a number of untracked objects, as well. Based on recent research (Oltrogge et al. 2018), there could be over 1600 objects between 10 cm and 1 m in size and 33,000 objects larger than 1 cm that cross the GEO protected region. The reference argues that a collision of a small, untracked 1 cm-class object with an operating satellite might occur as frequently as every 4 years and every 50 years for an object larger than 20 cm. In the GEO region, collision velocities could reach as high as 4 km/sec with objects in highly eccentric orbits piercing the GEO protected region. More common collisions would be at relative velocities of less than 1 km/sec.

One of the largest and oldest GEO operators is Intelsat, now a commercial company but originally established as an intergovernmental consortium in the 1970s. Intelsat currently operates a fleet of 52 communications satellites. The operating GEO satellites are large, and they have long lifetimes, some exceeding 30 years. Their locations are known well, and many of the satellites operate in orbits very near to Earth's equatorial plane, so they move slowly relative to one another. As a result, operators of GEO satellites generally have more time to make adjustments to avoid close approaches with known objects and maintain their satellites' orbital positions than those in LEO.

Satellites in GEO can provide services to a relatively large area of the Earth's surface, and their 24-hour orbits essentially fix them in place over specific points on the equator, so ground antennas can be pointed at predefined locations to send and receive signals. Satellites in GEO are designed to be very reliable and to operate within predefined slots for long periods. In the past, very large ground antennas were required for communicating with these satellites. The size requirements have been

reduced substantially over time. An antenna on a home or business that is pointing to the sky is generally pointing to a satellite in a GEO orbit.

For the near-term, major changes in the design and operational characteristics of GEO satellites or the GEO environment are not expected. An area where we might expect advancements is in the maintenance and disposal of GEO satellites, and some commercial companies are developing satellite servicing and potentially active debris removal (ADR) services as well. These services would perform satellite refueling and disposal services, potentially extending the life of operational satellites by replenishing station-keeping propellant and offering disposal options when satellites fail or end their missions. Since longer lifetimes have economic benefits to the owners, satellite operators could pay for servicing and disposal services. In the future, GEO operators might create a fund that would cover costs of removal of existing derelict satellites or satellites that fail prematurely.

For the GEO region, satellites are to be disposed in orbits above the GEO protected region where they will not reenter that region for at least 100 years. Design of disposal orbits must account for the long-term effects of solar wind, the gravitational attraction of the sun and moon, and other small forces.

## **LEO Protected Region**

Satellites in LEO are at lower altitudes (altitudes less than 2000 km), so their coverage on the Earth's surface is less. They do not operate over fixed regions of the Earth surface but make a complete orbit around Earth in 90 to 120 min. If services are desired by a customer at a fixed location, orbits must be designed to pass within range of that spot at prescribed intervals; if continuous communications is required, a constellation of LEO satellites is necessary, and multiple satellites in that constellation must provide coverage and make and hand off connections with that customer as services are provided. The communications pathway is completed by ground antennas that receive data from linked satellites and pass that data to ground-based users.

Since they are at lower altitudes, LEO satellites have the advantages that they require much less power to communicate with customers on the ground than satellites in GEO. That makes the individual satellites much less expensive to fabricate and put into orbit and enables a customer on the ground to use a low-power, hand-held instrument for communications. The communications time lag is also substantially lower, which is important for machine-to-machine communications.

These features were incorporated in the design of the Iridium satellite system, which includes a relatively large constellation of 66 satellites in low Earth orbit plus several on-orbit spares and provides voice and limited data communication to people located anywhere on Earth. All satellites in the Iridium constellation are essentially of the same design, enabling production on an assembly line. Iridium's first constellation became operational in 1998 and is now being replaced with more capable satellites.

Following Iridium's lead, a revolution is on the horizon as new operators propose very large constellations in the LEO regime. But given the realities illustrated in

Figs. 2 and 3, the environment in LEO – and on the ground – must be considered carefully as this revolution moves forward.

Over 1800 satellites currently operate in the LEO regime, joined by over 13,000 debris objects large enough to be tracked (i.e., larger than 10 square centimeters) plus possibly over 500,000 objects between 1 and 10 cm in size that are harmful to operating satellites but can't currently be tracked. In addition to the large population of orbiting objects, LEO is a more challenging environment than GEO for space operators for several reasons:

- Satellite orbits in LEO are affected by aerodynamic forces that are amplified by environmental factors such as the day/night cycle, solar storms, carbon dioxide in the environment, and other factors that make accurate predictions of where the satellites will be in the future much more challenging.
- For an object to be tracked, it must pass over tracking radar sites on the ground, which will limit the frequency of updates available of the object's orbit. These updates are required to correct for the effects of the atmosphere and other forces on the object's orbit. Without frequent updates, the uncertainty in an object's position at a given time increases, affecting the quality of a collision warning.
- While there are exceptions, operating satellites in the GEO protected region are taking advantage of circular orbits that are at very low inclinations, and positions are well known and well controlled, so most operating satellites move slowly relative to each other compared to those in LEO, where operating satellites are in multiple orbit planes and approach velocities for objects in different planes can be 10 km/sec or higher. As a result, a collision in LEO, even with a small debris object, can destroy an operating satellite and add large numbers of debris objects to the orbital environment.
- There are lots of dead satellites and other debris in LEO that must be frequently tracked, can't maneuver, and must be avoided.

As noted, orbits of satellites in LEO are affected by very small aerodynamic forces that increase as altitude decreases. While these forces help remove debris in low orbits, the lifetime of orbits increases substantially with altitude. For example, the orbit of a dead satellite in a 250-km circular orbit will decay, and the object will reenter in less than a year; a dead satellite in a 1000-km orbit will remain in orbit and be a hazard to other satellites for over a thousand years. Lifetimes of circular orbits continue to increase as altitude increases. Estimates of the lifetime for a particular satellite depend on the satellite's mass, physical dimensions, orientation, and environmental factors such as solar activity as it descends.

## Space Debris

Inoperable, human-made objects orbiting Earth are space debris, and space debris can be created by collisions and explosions, by release of objects during satellite deployments and normal operations, by strikes by micrometeoroids and small space debris fragments,

and by long-term exposure to the orbital environment. A collision or explosion involving a large object such as a satellite or launch stage creates an expanding cloud of debris objects that eventually blends into the background of debris objects in the orbital environment, slightly increasing the background risk to all satellites in the region. Traveling at orbital speeds, even a flecks of paint can gradually degrade solar panels and damage optical sensors, reducing the mission lifetime of the damaged vehicle. It should be noted that satellites with no maneuver capability are effectively space debris to an operating satellite, which must move to avoid a collision.)

Current guidelines and standards require that satellites in both the LEO and GEO protected regions remove themselves at end of mission to minimize the growth of space debris and minimize the possibility of interfering with other operating satellites in those regions.

At end of life, satellites in LEO orbits should be reentered into the atmosphere for disposal. The reentry process does not necessarily completely “burn up” a reentering object, and some fragments that are potentially hazardous to people on the ground can survive. For this reason, requirements state that if the casualty expectation per reentry exceeds 1 in 10,000 (i.e., surviving fragments might injure or kill one person on Earth should the object reenter 10,000 times), the object should be directed to reenter into a region where there is minimal hazard to people (e.g., an open ocean area). Otherwise, the object may be allowed to simply reenter as its orbit decays – as long as that process takes fewer than 25 years. (As will be discussed later, requirements to minimize hazards due to reentries of large numbers of satellites from large constellations may be a possibility for the future.)

The approximately 20,000 objects included in the figures are only those tracked by ground and optical sensors, and these generally range from 10 cm and larger in the LEO regime to 1 m and larger in the vicinity of the GEO regime. As noted, the orbital environment includes many thousands of objects smaller than 10 cm in size that have resulted from satellite explosions, collisions, debris expelled during normal operations, and other sources over the years. As a result, the total population of orbiting objects is actually considerably higher than the figures indicate, with estimates that the actual total includes as many as 500,000 small, currently untrackable (due to their size) objects in LEO, each of which is large enough to seriously damage a satellite on impact.

The jumps in the population of LEO objects shown in Fig. 1 are due to debris created by the 2007 Chinese anti-satellite (ASAT) test, where a ground-launched vehicle impacted an aging Chinese weather satellite, and collision of the active Iridium 33 satellite and inoperative Russian Cosmos 2251 satellite in 2009. The latter collision ended the operations of the Iridium satellite and also created a debris cloud that included several thousand additional objects, many of which will remain in orbit for decades to come. While some debris from these events has subsequently reentered and is no longer in orbit, Fig. 1 shows that many of the larger tracked objects (and likely many smaller, currently untrackable objects) remain in orbit. And given the altitude where the events occurred, some of these objects will remain hazards to other objects for centuries to come.

The Iridium-Cosmos collision changed the perspective on orbital risks and resulted in a new focus on providing better information to satellite operators on possible threats to their space assets.

## Space Situational Awareness Services

Prior to the Iridium-Cosmos collision, the “big sky” perspective, which said that space was so vast that collisions would be very rare, prevailed. Only a few satellite operators felt the need for real collision avoidance and other space situation awareness (SSA) services.

At that time, services were provided by the US Air Force using tracking data collected using government-owned sensor systems. And many operators felt that the available services were not “actionable,” meaning that predictions informed a satellite operator when an object might pierce the physical space surrounding a satellite, but that space could be kilometers in size. Given that level of uncertainty, operators did not feel there was sufficient information to warrant moving a satellite, since moving requires expenditure of propellant, with each maneuver fractionally reducing a satellite’s lifetime. And a move based on inaccurate data might actually increase the risk of a collision with the approaching object or possibly with another at a later time. Moving a satellite can also affect its ability to fulfil its basic mission objectives. For example, if a satellite must maneuver to avoid a possible collision, its ground coverage area will also move, potentially requiring operator actions to avoid loss of valuable data or service interruptions.

Over the years, new sensors and analysis techniques emerged. Shortly after the Iridium-Cosmos collision, the USA provided close approach distances and probabilities of collision to satellite operators. While this is an improvement over earlier formats for conjunction assessments, some satellite operators still felt that the information from the USA was insufficient for their needs.

In 2009, several operators of satellites in GEO orbits formed the Space Data Association (SDA) to “improve the accuracy and timeliness of collision warning notifications. . . via sharing of operational data.” The SDA, through its Space Data Center, supplements catalog data from the US government with information provided by operators of GEO satellites, who generally know very accurately where their satellites are and also know when satellite maneuvers will occur. The SDA also provides radio frequency interference and other support and assists operator efforts to coordinate maneuvers to avoid interference with other objects.

Today, in addition to the SDA and the US Air Force, several governments provide similar services for operators of their own satellites. But most use the US catalog of resident space objects, supplemented with information from their own sensors and satellite operators, as the basis for their services.

## Space Situational Awareness Data

Since the beginning of the space age, the primary catalog used for SSA services has been created and maintained by the US Air Force. This Resident Space Object (RSO) catalog is generally considered to be the most complete of any currently available, and unclassified portions of this catalog have been made available for years ([Space-Track.org](#) is the current source). Data for this catalog has been collected

primarily by ground-based radar and visual telescope systems operated by the US government. Planned enhancements to tracking resources may decrease the minimum size of tracked objects to as small as 2 cm. As a result, the number of objects in the RSO catalog is expected to increase from approximately 20,000 to over 200,000.

At present, new commercial and international entities are adding their data to the mix. For example, one company currently has two phased-array radar sites in operations and is building a third. That company is currently tracking more than 14,000 objects in LEO and expects to track as many as 250,000 objects 2 cm and larger several times a day when its radars are fully deployed and operational. A second company is operating a global SSA telescope network with more than 25 observatories and 250 telescopes that is tracking man-made space objects in GEO, highly elliptical orbits (HEO), and medium Earth orbits (MEO). Both of these companies offer a variety of services based on the data they collect.

Collecting data on most objects several times a day will enable space situational awareness services of unprecedented accuracy. This type of data will be essential as SSA service providers, who will need to provide accurate and timely warnings of collisions and other interference as the number of objects increases over the next 10–20 years.

## Best Practices and Standards

As the number of objects in orbit increased, it became apparent that best practices, guidelines, and even regulations were required to prevent the growth of the space debris population. If this was not done, predictions were that the debris population could continue to increase in an uncontrolled manner as objects and fragments of objects impacted other objects, creating more fragments, etc. (the Kessler effect), eventually making space operations much more difficult and expensive.

And even small, untracked debris can cause problems. For example, impacts of a small debris particle on a solar panel can reduce the power output from that panel – and a large number of impacts can drop the power output so low that the satellite is not able to perform its designated mission and must be deorbited. Ailor (2010) concluded there would be a relatively small decrease in the mean satellite lifetime due to operating in the debris environment for the next 30 to 50 years based on the then-projected environment (an environment with no very large constellations in LEO). A primary driver in the lifetime reduction was the solar panel degradation due to impacts by small debris – impacts that gradually lowered the power provided by the solar panels until power dropped below a critical value, ending the satellite’s mission. The effect of the addition of large LEO constellations on these projections will be discussed later.

During this period, it was also recognized that when a launch vehicle or spacecraft reentered the atmosphere at end of life, the object would not completely “burn up.” Fragments that could injure or kill a human on the ground might survive.

In the late 1990s, the Inter-Agency Space Debris Coordination Committee (IADC) developed guidelines stating that satellites in LEO should be disposed



before their end of life, either by moving them to an orbit that would naturally decay in 25 years or less or preferably by direct reentry – controlling the deorbit process so the debris surviving reentry lands in a safe area. Direct reentry into the atmosphere was recommended for objects where surviving debris might have casualty expectations exceeding 1 in 10,000 (i.e., reentries of that object 10,000 times would be expected to cause one casualty somewhere on Earth). Many nations have incorporated these guidelines into regulations.

The IADC guidelines were developed for reentries of individual satellites. Current proposals suggest that several constellations containing many satellites may be in the offing for the next decades. As will be discussed later, this may lead to new guidelines designed to limit the creation of space debris and hazards to people on the ground and in aircraft as we move forward.

---

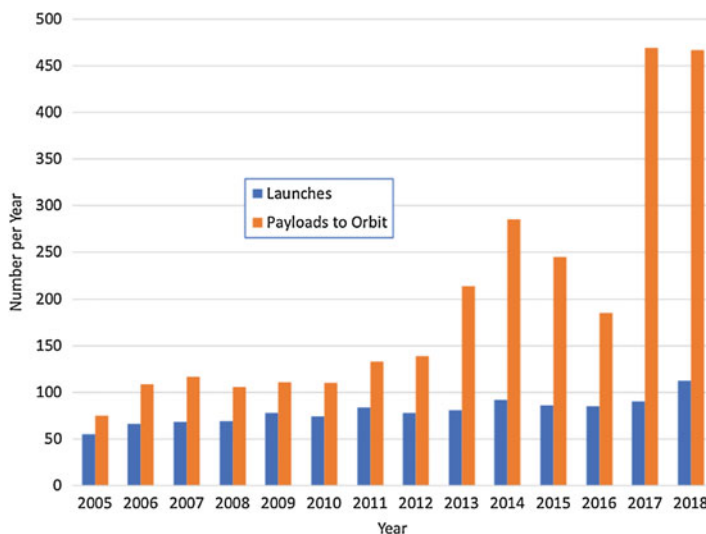
## Changes Coming

From the beginning of the space age to the early 1990s, satellites were essentially one-of-a-kind items – each was built with specific capabilities designed for specific missions, and each launch carried only one or, at most, two satellites to orbit. The Iridium satellite system changed that paradigm with its factory-built satellites. The release of the iPhone in June 2007 was another paradigm shifter and was described as “revolutionary” and a “game changer” for the mobile phone industry. These events and subsequent releases of smart phones that included small accelerometers, sensors, cameras, microprocessor, and other technologies encouraged innovators to see how these new satellite manufacturing processes and microelectronics capabilities might be used more broadly in space systems.

During this period, a standard size for a new class of small satellites was defined – a cube  $10 \times 10 \times 10$  cm in size – and launch service providers included “piggyback” launchers for these CubeSats that could deploy many such satellites per launch. Most of these small satellites were placed in the low Earth orbit regime, and many were low enough that their orbits would decay within a few years – an important feature given the increasing recognition of a growing space debris problem. Very few of these satellites carried significant propulsion capabilities, and most were experimental in nature, so many rapidly became “space junk,” joining the population of nonfunctioning, human-made debris circling our planet.

These new technologies led to a decrease in cost and mass of very capable satellites, enabling providers of space-based services to consider providing worldwide communication and internet services via constellations consisting of large numbers of small satellites (satellites less than 500 kg) in LEO. These satellites would follow the approach used by Iridium: a large number of satellites based on a fixed design would be mass-produced on an assembly line.

A benefit of the smaller satellite size and mass is that launch vehicles could carry more than one satellite to orbit, and Fig. 5 shows the number of launches and the number of satellites carried to orbit per launch from 2005 through 2018. While the number of launches per year has been relatively stable, the number of payloads per



**Fig. 5** Number of worldwide launches and payloads carried to orbit from 2005 through 2018

launch has increased substantially (launch failures affected the number of launches and payloads to orbit in 2015 and 2016).

## Large LEO Constellations

The lower costs associated with satellite manufacture and launch have led to proposals for placing really large constellations of satellites in LEO, with some exceeding over 1000 satellites in orbit with multiple satellites in each orbit plane. Table 1 lists some organizations that have announced such plans.

The largest proposed constellation to date is SpaceX's StarLink constellation, which would have over 7500 satellites orbiting at 346 km (below the orbit of the International Space Station). If completed, that one constellation would have over four times the total number of satellites that were operating in orbit at the beginning of 2019. SpaceX has proposed locating another 4425 satellites at 1100–1300 km as part of that constellation. While some of the constellations in Table 1 may not materialize, it is evident that the LEO space environment may change dramatically over the next decades.

Clearly the addition of such large numbers of satellites into the LEO regime will raise a number of questions that should be answered. These include:

- 1. How will satellites in these constellations be delivered to their operational orbits?** Satellites can be inserted relatively quickly into their orbital positions by launch stages, a common practice today, or they may be inserted into a lower orbit, where they can be deployed, checked out, and then boosted to a higher

**Table 1** Proposed constellations

Proposed constellations	Number of satellites
SpaceX K-band (high altitude)	4425
OneWeb	720
LeoSat	120
Theia	112
Telesat	117
Boeing	2956
SpaceX V-band (low altitude)	7518

mission orbit. The advantage of the latter approach is that the checkout orbit can be low enough that the orbit will decay quickly if the satellite is faulty, minimizing the likelihood of subsequent failure and leaving a dead satellite at higher constellation altitudes. If the satellite is found to be healthy during checkout, it can then be put on course to its final orbit.

Some are considering using an electric propulsion system for the transfer from the low orbit to the constellation altitude. While this technique minimizes propellant consumption, it produces a very low thrust, so the satellite will move relatively slowly through altitudes where other satellites operate as it spirals upward, increasing the potential collision threat during transit and the load on operators of space traffic management systems as they seek to minimize the possibility of collisions.

2. **With so many satellites in a large constellation, how will risks to satellites passing through be managed?** In GEO, the International Telecommunications Union (ITU) assigns satellites to operate in specific orbital slots, typically two degrees in size, to minimize frequency interference problems. Since GEO satellites provide services over specific ground areas, these restrictions work well: operators of GEO satellites know whose satellites are operating where and announce moves and activities to avoid interference.

In LEO, the situation is different: satellites in LEO circle Earth about every 90 minutes and collect data and provide services over relatively small areas as they pass overhead. As a result, an operator wishing to add a satellite to a constellation at a higher altitude must coordinate the passage of that satellite with operators of constellations below that altitude. And if the satellite being moved uses low-thrust propulsion, the transit time will not be quick. The concept of assigning a constellation responsibility for its “shell” and providing best practices for operators wishing to pass through that shell has been suggested. No formal arrangements have been made along these lines.

3. **What is the expected lifetime of satellites in the constellation?** An advantage of the LEO constellations is that it is relatively inexpensive to launch replacement satellites that incorporate the latest systems and capabilities, so some constellation designers might use satellites with 5- to 10-year lifetimes. That could mean a large fraction of each constellation would be moving toward disposal each year as constellations are maintained. For example, assuming a 10-year lifetime, a large

fraction of the satellites could be moving down through lower altitudes toward reentry on a yearly basis. And if electric propulsion is used, that transit could take significant time. All of these satellites in transit to and from the constellations add to the risks of collisions in LEO, so satellite lifetime and constellation disposal plans and strategies will be important considerations as plans for constellations develop.

4. **What happens if a satellite fails while operating in the constellation?** It is inevitable that satellites operating in constellations will fail. These large constellations in low Earth orbit must necessarily have multiple satellites in each orbit plane to provide ground coverage to service their customers (e.g., there are 11 satellites in each of the 6 orbit planes in the 66-satellite Iridium system, and Iridium also maintains several in-orbit spares). A constellation with thousands of satellites could have a hundred or more satellites in each plane, and the operations of each must be well controlled and well-coordinated in orbit. If a satellite fails or communications is lost, it could become a threat to others in the same plane and in the constellation itself. Active support from a space situational awareness service would be required in this case. Clearly, satellites in constellations should be designed with very high reliability for disposal.
5. **How will satellites be disposed at their end of life?** The preferred approach for disposing satellites is to have them leave orbit and reenter the atmosphere in a location where surviving debris will impact in an uninhabited area such as the South Pacific Ocean. In this case, surviving debris has minimal chance of injuring a human or damaging an aircraft. As noted earlier, if the casualty expectation for a reentry is less than 1 in 10,000, current guidelines and regulations say that the satellite can simply be left in an orbit that will decay in less than 25 years. As large constellations emerge, regulators may choose to also limit the hazard posed by cumulative reentries of satellites from these constellations (more on this later). And the 25-year time allotment could be shortened to reduce the transit time to reentry, or might even be eliminated in favor of requiring direct disposal of satellites of larger sizes to minimize ground hazards arising from reentries of large numbers of satellites per year.
6. **How important is satellite disposal?** A key factor in determining the future of debris growth in LEO is the reliability of disposal at end of mission or end of life. Dead satellites in some constellations could remain a threat for hundreds or thousands of years, so managing the LEO environment will require satellites to have disposal systems that can deorbit constellation members with a very high probability of success – some argue the probability of success should be over 90% if we are to maintain some control on the growth of the LEO population.
7. **Since satellites from large constellations will be disposed by reentry into the atmosphere, will risks of hazards to people on the ground or in aircraft increase?** Studies are showing that yes, hazards to people on the ground and in aircraft could increase substantially as a result of hardware associated with large constellations reentering Earth's atmosphere. More on this later.
8. **How will the increase in space traffic be managed?** The current SSA system tracks 20,000 to 30,000 objects, and, as noted earlier, satellite operators in the

LEO regime are calling for services that provide more and more accurate information to help them protect their on-orbit assets. Upcoming improvements in ground-based tracking services may increase the number of objects tracked by a factor of 10. Satellite operators, SSA service providers, and government regulators must work together with regulators to develop best practices, standards, regulations, and policies designed to assure the long-term sustainability of space activities in the LEO environment.

So, given the advent of large LEO constellations, what challenges might be expected in efforts to maintain the long-term sustainability of the space environment and management of space traffic and limit potential hazards to spacecraft in orbit and people on the ground?

## **Environmental Effects on Satellite Lifetime**

The study conducted by Ailor et al. (2010) with no large constellations and assuming business-as-usual satellite operations, disposal, and replenishment activities found that large satellites operating in the LEO regime could experience a mean lifetime reduction over the next 50 years of about 13% (e.g., a satellite with a mean lifetime of 10 years in a no-debris environment would see a reduction of 1.3 years in an environment that included space debris). Much of this reduction would come from degradation of solar panels by small, untrackable debris that would “sandblast” and reduce the power output of solar panels.

An update to that study (Ailor et al. 2017) assumed that over 5000 new small satellites are operating in high LEO orbits, consistent with proposals announced by commercial companies in the 2015–2017 timeframe. As with the 2010 study, this projection included the effects of collisions of both tracked objects, objects greater than 10 cm in LEO, and small debris down to 1 mm and adds changes in the debris environment due to the previously un-modeled new satellites colliding in their constellations and with other objects as they undergo constellation replenishment activities.

Primary results were that satellites being disposed from or added to the new constellations and debris associated with collisions involving these objects could potentially double the reduction in the mean operational lifetime of satellites operating in LEO over that predicted under the business-as-usual approach. As in the 2010 study, the degradation of solar panels due to small debris impacts was a significant factor in this degradation, with the mean lifetime reduction increasing from the 13% predicted in the earlier study to as much as 60% in some cases (i.e., a large satellite with a mean lifetime of 20 years in a no-debris environment could have its mean lifetime reduced by as many as 12 years in an environment that included debris associated with constellation satellite operations). Results suggest that minimizing collisions during replenishment activities and making solar panels and space hardware more resilient to small debris impacts will be increasingly important in the future.

## Reentry Disposal of Satellites from Large Constellations

As noted earlier, current regulations limit the casualty expectation for a single satellite reentering in a random, uncontrolled manner to less than 1 in 10,000. If the predicted hazard exceeds that number, the satellite should be commanded to reenter into a safe area such as the South Pacific Ocean. The original Iridium satellites were predicted to each have a casualty expectation of 1 in 17,000, so random reentries were acceptable as the Iridium system evolved.

In 2000, Iridium was having significant financial problems, and as a part of bankruptcy considerations, the government asked that NASA develop an estimate of the cumulative hazard should Iridium be required to dispose all 74 of its satellites. The estimated *cumulative* hazard for reentering all 74 satellites was 1 in 250, well above the 1/10,000 limit for a single satellite. Fortunately, Iridium's financial problems eased, and the constellation has remained in operation. (Notably, satellites from the original constellation are gradually being disposed and replaced by the new Iridium Next satellites, and no fatalities from the disposal operations have been reported to date.)

Similar to the Iridium process, some current proposers of large constellations plan to dispose of their satellites at end of mission by lowering their orbits so random reentries into the Earth's atmosphere would occur within the 25-year timeframe.

A recent study (Ailor 2019) used the past history of debris surviving satellite reentries to develop a first-order estimate of the hazard to people and aircraft from falling debris that could survive reentries of constellation-sized satellites. Projecting to the year 2030, when several proposed constellations were assumed to be operational and were disposing a fraction of their satellites each year, the results show that hazards to people on the ground posed by debris from multiple satellite reentries from a single large LEO constellation could exceed the 1 in 10,000 threshold for a single satellite by 2 to 3 orders of magnitude.

That same study used radar observations of debris falling from a satellite reentry in the 1970s and US departures and destinations of 17 types of large, commercial aircraft to estimate the probability of hazardous debris striking an aircraft given possible masses of satellites proposed for a LEO constellation would be 0.001, corresponding to a maximum yearly casualty expectation for reentries from a single large constellation of nearly 3 in 10 without emergency action by a pilot after such an impact. That estimate would be higher if commercial air traffic was updated to include worldwide flights.

It should be noted that while reentry hazard prediction models can be verified to some degree based on recovered debris (Ailor et al. 2011) and actual data collected during breakup (Feistel et al. 2013), there is very little data on small objects that might survive and be a hazards to aircraft. As large constellations evolve, satellite designs that minimize the number and size of surviving debris should be considered, as should means to verify that the designs are performing as predicted.

To summarize, there are currently no guidelines or requirements to manage cumulative risks for either ground or aircraft casualties. While new satellite design practices might lower the number of hazardous fragments that result from reentries, the most effective mitigation technique would be to deorbit all satellites into a safe ocean area.

## Active Debris Removal (ADR)

Systems are being developed for servicing satellites in GEO orbits, and these systems might also be used to move satellites from the GEO protected region to disposal orbits. There is a potential market for satellite servicing given the “more civilized” operating environment in GEO, where a servicing vehicle could visit several operating satellites travelling in virtually the same orbit. Satellites operating in GEO are generally more expensive to build and launch and are designed with long lifetimes, so servicing that extends a satellite’s lifetime could be less expensive and more cost-effective than replacement in some cases.

As noted, the LEO operating environment is different, with satellites operating in multiple orbits with inclinations varying from near zero to over 90 degrees. In addition, satellites are smaller and less expensive to build and launch and offer the advantage that new technologies can be infused quickly by replacing older satellites with newer versions. As a result, while proposals using electrodynamic tether systems and other approaches have been suggested for removal and a new company has announced plans to develop and demonstrate ADR technologies to approach and capture space debris, satellite servicing has not been a potentially attractive market in LEO to date.

But, the addition of new LEO constellations with large numbers of satellites in roughly the same orbits could encourage a new look at LEO satellite servicing and removal, perhaps as part of a constellation’s design. For example, given the possibility that new requirements might emerge that would limit the cumulative hazard posed by reentry disposal of satellites from a constellation, constellation designers might include satellites specially designed to remove and dispose of dead satellites or satellites that have reached their end of life via direct disposal into a remote area. And given that a large constellation could have many satellites in the same orbit and orbit plane, a servicer could replace or update components in multiple satellites as an alternative to totally replacing those satellites.

In addition, the LEO environment currently includes several very large, dead satellites and rocket stages that will remain in orbit for many years. Should any of these be impacted by another debris object or an operating satellite, the number of debris objects created could be much larger than that from the Iridium-Cosmos and the Chinese ASAT tests. These objects should be priority targets for an ADR system. To encourage development of ADR capabilities, the International Association for the Advancement of Space Safety (IAASS) has proposed an international grand challenge for ADR (Position Paper [2017](#)).

## Effect of Large Constellations on SSA Service Requirements

As noted earlier, space situational awareness services (e.g., predicting close approaches that might threaten an operating satellite) are currently based on databases of some 20,000 objects. New tracking services will increase the size of these catalogs by a factor of at least ten as currently existing small objects, objects from 2

to 10 cm in size, are added. Objects in this size range are capable of seriously damaging or ending the operational lifetime of a satellite.

Recent studies (Peterson et al. 2018) are showing that, using current practices, the addition of large constellations plus the large numbers of satellites transiting the LEO regime as they dispose and replace satellites in these constellations are likely to increase the number of conjunction alerts sent to satellite operators to possibly over 1000 alerts per day. Many of these would not be alerts if tracking uncertainties on all orbiting objects, both operating satellites and hazardous debris objects, were reduced. Installing tracking aids such as transponders on operating satellites and including satellite owner/operator data in conjunction assessments will improve the situation somewhat, but given that debris dominates the population of orbiting objects in LEO, only basic improvements in the tracking accuracy for all objects and in information provided to operators by space situational awareness services will improve the situation substantially.

## **Space Situational Awareness and Traffic Management Service Providers**

As noted earlier, the major provider of SSA services and space tracking data to date has been the US government via the US military. The military manages the collection of data from US-owned ground-based and optical sensors and processes this data to provide conjunction assessment services to satellite operators around the world and basic data to the public. But changes are coming.

The growth in the number of nongovernment satellites and satellite operators is placing an increasing demand on the current military operations, and in response, responsibilities for providing these services may be transferred to a civil agency within the US government. A new civil space traffic management (CSTM) system would likely maximize the use of commercial capabilities and data sources to provide enhanced SSA services as a public good (i.e., at no cost) and could make data available to support the development of specialized, higher level support by commercial entities.

The migration of basic space situational awareness capabilities from the Air Force to a new CSTM entity will likely be complete in the early to mid-2020s. Given its responsibilities, the new organization, likely using data that includes data from commercial data providers, will play an increasingly important role in protecting the near-space environment and shaping the standards, best practices, and regulations that will guide space operations for decades to come.

---

## **Conclusions**

Specific areas where new services, best practices, standards, and regulations are likely to evolve are:



- **Minimizing the growth of space debris:** Unfortunately, the LEO regime already has a large population of uncontrolled debris objects that can collide with other objects and generate more long-lasting debris. The addition of large numbers of new satellites as large constellations are inserted and maintained has the potential to make operations in LEO much more expensive, forcing satellite designs that are more robust to small debris impacts and have very reliable systems for deorbit at end of mission or after an on-orbit failure. In addition, it is likely that guidelines will be developed encouraging operators of large constellations to deorbit satellites at end of mission quickly, possibly within 5 years or even via direct disposal, to minimize the possibility of collisions. It should be noted that active debris removal could also play an important role: removal of one large, dead satellite or launch stage could eliminate a potential source of debris objects equivalent in number to that possible by decades of mitigation.
- **Providing services to satellite operators:** Services that alert satellite operators of an approaching threat will have a critical role as the number of tracked objects increases due to addition of hundreds of thousands of existing small and hazardous debris objects and satellites associated with large constellations are added to SSA databases. Satellite operators need predictions that are accurate and timely to avoid unnecessary moves. Fortunately, commercial data providers are emerging that promise data that meet necessary requirements, and it is expected that this data will reduce the overall number of alerts to satellite operators. At the same time, the nature of the service providers will also change as providers for SSA and space traffic management services enhance their predictions by incorporating data acquired from commercial entities. Services provided by the US government are sure to evolve as they move from the US military to a civil agency. Active debris removal and satellite servicing may evolve as cost-effective ways to maintain GEO satellites. Similar systems could emerge to maintain and update satellites in large LEO constellations.
- **Addressing needs of governments and regulators:** There will be increased attention to the space environment as proposals for large constellations are realized over the coming years. And if a serious collision occurs, governments will be more likely to collect and analyze data to assure that operators are abiding by agreed restrictions. Governments are also more likely to support regulations to assure that current and future space operators have reasonable access to space and minimal interference with space operations.
- **Assuring safe on-orbit operations and disposal of space systems:** Collection, maintenance, and sharing of accurate data required for assessing possible conjunctions involving all orbiting objects larger than 2 cm will be increasingly important. Included will be sharing of data among satellite operators and space traffic management service providers. This data will be essential for services that provide timely, accurate services to prevent conjunctions among operating satellites and debris and assist with anomaly resolution and mission planning. In addition, the spacefaring community will need to verify proposals that would limit casualties on the ground and in aircraft via “design for demise” techniques and potentially develop cost-effective techniques that will enable direct disposal

of space hardware into safe areas. Finally, practices that minimize interference to satellites and launching systems transiting shells where large constellations are operating need to be developed.

The addition of large constellations of satellites to the LEO environment presents the opportunity to, in effect, re-architect LEO operations for the future. For the last 50 years, satellite operators have operated essentially unfettered by regulations on where they can operate, how they can maneuver, or concepts of “ownership” of a particular region of space. The introduction of thousands of new satellites to this region will make the development of best practices and possibly imposition of restrictions and limitations on where and how satellites can operate necessary if humanity is to preserve that environment for the future.

---

## References

- Ailor W (2019) Hazards of reentry disposal of satellites from large constellations. *J Space Safe Eng* 6:113–121
- Ailor W, Womack J, Peterson G, Lao N (2010) Effects of space debris on the cost of space operations. In: IAC-10.A6.2.10, 61st International astronomical congress. Czech Republic, Prague, 27 Sept–1 Oct 2010
- Ailor WH, Hallman WP, Steckel GL, Weaver MA (2011) Test cases for reentry survivability modeling. In: 5th IAASS conference, Versailles, 17–19 Oct 2011
- Ailor W, Peterson GE, Womack J, Youngs M (2017) Effect of large constellations on lifetime of satellites in low earth orbits. *J Space Safe Eng* 4:117–123
- Feistel AS, Weaver MW, Ailor WH (2013) Comparison of reentry breakup measurements for three atmospheric reentries In: 6th International association for the advancement of space safety conference, Montreal, May 2013
- ISO 24113 (2019) Space Systems - Space debris mitigation requirements. Reproduced with permission of International Organization for Standardization, ISO. Standard available from any ISO member or see <http://www.iso.org>. Copyright remains with ISO
- Oltrogge DL et al (2018) A comprehensive assessment of collision likelihood in geosynchronous earth orbit. *Acta Astronaut* 147:316–345
- Peterson GE, Jenkin AB, Sorge ME, McVey JP (2018) Tracking requirements for space traffic management in the presence of proposed small satellite constellations. In: IAC-18,A6,7,6, x43991, 69<sup>th</sup> international astronomical conference, Bremen, 1–5 Oct 2018
- Position Paper (2017) A grand challenge for active removal of space debris In: International association for the advancement of space safety, IAASS-PP-00117-WA, 17 May 2017. See <http://iaass.space-safety.org/wp-content/uploads/sites/24/2018/03/Orig.-Position-Paper-on-ADR-v6-1.pdf>



Peter Martinez

## Contents

Space Security and Space Sustainability .....	320
Space Security .....	320
Space Sustainability .....	321
The United Nations and Space Sustainability .....	322
Space in the UN System .....	322
The United Nations Committee on the Peaceful Uses of Outer Space .....	323
COPUOS and Space Sustainability .....	325
Introduction of the Long-Term Sustainability of Outer Space Activities on the Agenda of COPUOS .....	325
COPUOS Working Group on the Long-Term Sustainability of Outer Space Activities ...	326
The Guidelines .....	331
Implementation and Updating of the Guidelines .....	333
Other Multilateral Initiatives with a Connection to Space Sustainability .....	334
Conference on Disarmament .....	334
UN Group of Governmental Experts on Transparency and Confidence-Building Measures (TCBMs) in Outer Space Activities .....	335
The EU Proposal for an International Code of Conduct for Outer Space Activities .....	336
Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space .....	337
Concluding Remarks .....	338
References .....	339

## Abstract

Space sustainability is a concept that has emerged within the past 15 years to refer to a set of concerns relating to outer space as an environment for carrying out space activities safely and without interference, as well as to concerns about ensuring continuity of the benefits derived on Earth from the conduct of such

---

P. Martinez (✉)  
Secure World Foundation (SWF), Broomfield, CO, USA  
e-mail: [pmartinez@swfound.org](mailto:pmartinez@swfound.org)

space activities. As such, it encompasses the concerns of both space actors and those who are not space actors but who nevertheless benefit from space activities. This chapter reviews the role of the various relevant United Nations entities in ensuring space sustainability and provides a detailed review of the process and discussions held in the Working Group on the Long-Term Sustainability of Outer Space Activities within the Scientific and Technical Subcommittee of the United Nations (UN) Committee on the Peaceful Uses of Outer Space (COPUOS). Finally, the chapter discusses the relationship of the work in UN COPUOS with related work done in the Conference on Disarmament, the UN Group of Governmental Experts (GGE) on Transparency and Confidence-Building Measures in Outer Space Activities, and the initiative by the European Union to propose a Draft International Code of Conduct for outer space activities.

---

## Space Security and Space Sustainability

The terms *space security* and *space sustainability* are sometimes used interchangeably to encompass a set of largely overlapping concerns as seen from two somewhat different perspectives. Underlying both of these perspectives is the acknowledgment that space systems underpin the modern information society and now form part of the critical infrastructure of most nations, whether they are spacefaring or not, and that this infrastructure is exposed to a series of risks of natural and anthropogenic origin. Regardless of the perspective from which one sees the problem, the point is that coordinated global action will be required to address these concerns. Acknowledging and addressing these different perspectives is one of the challenges that will be faced by multilateral initiatives to promote either space security or space sustainability. Hence it is instructive in the context of this chapter on space sustainability in a book devoted to space security to elaborate on this issue of the two perspectives.

### Space Security

*Security* is, in general terms, about being free from danger or threat. In practical terms, this means freedom from doubt, anxiety, or fear based on well-founded confidence that there are mechanisms and processes in place to ensure security as a condition.

However, attempts to pin down exactly what is encompassed by the word *security* prove to be elusive as there is no single universally accepted definition of the concept of “security.” In some countries the understanding of the term encompasses human security, environmental security, food security, and so on, while in others the term has a narrower meaning, referring primarily to military and defense-related issues.

*Space security* is a term that is used among space actors to refer to preserving order, predictability, and safety in space and avoiding courses of action that would ultimately undermine mission assurance, operational safety, and freedom of action in outer space. Another key dimension of this dialogue is the notion that, because

of growing reliance on space systems in every facet of modern life, security on Earth (regardless of how one defines it) is increasingly underpinned by security in outer space. Hence one of the key aims of the space security dialogue is to ensure freedom from threats (either ground-based or space-based) to the effective access to and utilization of outer space. For some actors this is closely coupled to concerns about the potential weaponization of outer space, although it is difficult to progress beyond a general acknowledgment of the potential problem to practical measures to avoid it, because of disagreements around the definition of what constitutes a space weapon.

An important point to note is that the space security discourse has, up until recently, been dictated by the national interests and concerns of the major space powers, who are the ones who most heavily invested in space-based infrastructure to support their national security. For some sitting on the sidelines of the debate, space security has sometimes been perceived to be predominantly the preoccupation of the advanced space actors and thus far-removed from the day-to-day concerns of the non-space nations. Others, particularly those from emerging or aspiring space nations, have seen the promotion of multilateral space security discussions as an attempt by the leading space actors to advance and preserve their national space interests and advantages by raising entry barriers to aspiring newcomers on the pretext that the space environment is already “saturated” with actors. Neither of these perceptions has helped to build multilateral consensus on normative rules of behavior for all space actors. However, there are promising signs of middle space powers beginning to play a more active role in promoting multilateral space security dialogues in the future and hence helping to bridge the gap between these different perceptions of space security.

## Space Sustainability

The word *sustainability* is derived from the Latin verb *sustinere* (*tenere*, “to hold”; *sus*, “up”) and is usually used in the context of being able to maintain an activity at a certain rate or level. Since the 1980s the concept of sustainability has been applied to human habitation and utilization of planet Earth and its resources. This has given rise to the widely used term *sustainable development*. This term was coined in the book *Our Common Future*, which contains the report published by the Brundtland Commission in 1987 (UN GA 1987). The definition for sustainable development given in that book is worth quoting here:

*development that meets the needs of the present without compromising the ability of future generations to meet their own needs.*

Notice the emphasis on “needs” in this definition. The Brundtland Commission’s report placed emphasis in particular on meeting the essential needs of the world’s poor, rather than satisfying the nonessential desires of the well-to-do.

The connection of *sustainability* with *outer space* arises from the perspective that space systems are now major global utilities that meet various societal needs. When

seen in this light, *space sustainability* is understood to be about using outer space in such a way that all humanity will be able to continue to use it in the future for peaceful purposes and for societal benefit. The sustainability concern here is driven by the realization that the Earth's orbital environment and the electromagnetic spectrum are limited natural resources. This realization leads naturally to a concern for how to ensure that the benefits of space activities will continue to be accessible to future generations and to all nations and raises issues about the equitable and responsible access to and use of space resources.

In other words, from this perspective, space sustainability is seen in the context of wider sustainability discussions and is perceived to be the concern of all beneficiaries of space activities. It is thus an intrinsically multilateral issue. This is a significantly and fundamentally different point of departure for addressing a very similar set of issues driving the space security discourse.

---

## The United Nations and Space Sustainability

The space arena today encompasses a much larger and much more diverse group of space actors than was the case in the first few decades of the space age. These include the “traditional” space actors, such as national space agencies and other national civilian agencies and the military, and a growing number of non-state actors, such as private sector commercial entities, academic and research institutions, and civil society organizations. We are also seeing the emergence of new kinds of space activities, many of which involve operations of space objects in close proximity to each other. Since the actions of a single actor can have consequences for all other actors, no single country (or even a group of like-minded countries) can control the space environment by its (or their) behavior or power alone; collective multilateral action is required.

In terms of international space law, states bear international responsibility for all space activities, including the activities of non-state entities (Outer Space Treaty 1967: Article VI). Hence, in spite of the growing number of non-state actors, the United Nations as a forum for states remains the relevant international forum to discuss such issues. Notwithstanding the preeminent role of states in the legal framework for outer space activities, it is worth reflecting on the contribution of civil society to the discussion on space sustainability, since this sector is playing an increasingly prominent and catalytic role in space activities and is in some respects more responsive to the rapidly changing space arena than the “traditional” fora established by states. This sector also has the access to a great deal of expertise, particularly in the conduct of space operations.

### Space in the UN System

At present, there are four principal fora at which space issues are discussed multilaterally in the UN system: (i) the United Nations Committee on the Peaceful Uses of

Outer Space (COPUOS) in Vienna; (ii) the Conference on Disarmament (CD) in Geneva; (iii) the UN General Assembly in New York (and two of its committees, the Disarmament and International Security Committee (First Committee) and the Special Political and Decolonization Committee (Fourth Committee)) ; and (iv) the International Telecommunications Union (ITU) in Geneva, which deals with spectrum and geostationary orbital slot assignments. In addition to these, the World Meteorological Organization in Geneva makes use of space systems for monitoring and predicting terrestrial weather and also supports international coordination of space weather activities, an area of growing importance since space weather affects all space systems.

Space is widely used in the UN system and its entities. Each year approximately 20 UN entities and specialized agencies hold the United Nations Inter-Agency Meeting on Outer Space Activities. They discuss matters of mutual interest in the applications of space technologies to address human needs. Considerations include the implementation of the recommendations of the UNISPACE conferences and space-based contributions of the United Nations entities to the achievement of the Sustainable Development Goals as well as to the implementation of the recommendations of various world summits. The meeting issues a report on its deliberations for the consideration of COPUOS.

## **The United Nations Committee on the Peaceful Uses of Outer Space**

The United Nations Committee on the Peaceful Uses of Outer Space (COPUOS) is the principal international forum for the development and codification of laws and principles governing activities in outer space. It is a standing committee of the UN, established in 1959 by 24 member states and given its mandate in UN General Assembly resolution 1472 (XIV). The Committee currently comprises 95 member states and a large number of permanent observers that enrich its work. The technical work of COPUOS is carried out by two subcommittees, the Legal Subcommittee (LSC) and the Scientific and Technical Subcommittee (STSC). Decisions in COPUOS and its subcommittees are reached by consensus. The Secretariat of COPUOS is the UN Office for Outer Space Affairs (UN OOSA), which is situated at the United Nations Office in Vienna.

During the 60 years of its existence, the deliberations in COPUOS have resulted in a number of very positive developments to advance international cooperation in the peaceful uses of outer space. A full discussion of all the activities and outcomes of COPUOS is outside the scope of this chapter, but it may be found in the paper by Hedman and Balogh (2009). Here, we focus on the aspects of COPUOS pertaining specifically to the long-term sustainability of outer space activities.

## **The International Legal Framework for Space Activities**

COPUOS is the only international forum for the development and codification of international space law. Since its inception, the committee has concluded five

international treaties and five sets of legal principles governing space-related activities. The five United Nations Treaties are:

- *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* (known as the “Outer Space Treaty”), adopted by the General Assembly in its resolution 2222 (XXI), opened for signature on 27 January 1967, entered into force on 10 October 1967;
- *Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space* (known as the “Rescue Agreement”), adopted by the General Assembly in its resolution 2345 (XXII), opened for signature on 22 April 1968, entered into force on 3 December 1968;
- *Convention on International Liability for Damage Caused by Space Objects* (known as the “Space Liability Convention”), adopted by the General Assembly in its resolution 2777 (XXVI), opened for signature on 29 March 1972, entered into force on 1 September 1972;
- *Convention on Registration of Objects Launched into Outer Space* (known as the “Registration Convention”), adopted by the General Assembly in its resolution 3235 (XXIX), opened for signature on 14 January 1975, entered into force on 15 September 1976;
- *Agreement Governing the Activities of States on the Moon and Other Celestial Bodies* (known as the “Moon Agreement”), adopted by the General Assembly in its resolution 34/68, opened for signature on 18 December 1979, entered into force on 11 July 1984.

The 1967 Outer Space Treaty laid the general legal foundation for the peaceful uses of outer space and provided a framework for developing the law of outer space. The four other treaties deal more specifically with certain concepts contained within the Outer Space Treaty.

It is instructive to review some of the principles in these treaties that provide the legal context for discussions on space sustainability and space security. These include the non-appropriation of outer space by any country; the freedom of exploration, scientific investigation, and the use (and even exploitation) of natural resources in outer space; state liability for damage caused by space objects; the avoidance of potentially harmful interference with space activities of other states; the sharing of information on space activities; and the registration of space objects.

The treaties affirm the agreement of states that the domain of outer space is a *res communis* and that the activities carried out therein and the benefits arising therefrom should be devoted to enhancing the well-being of all countries and humankind. Article I of the Outer Space Treaty is of particular relevance to the space sustainability discussion:

*The exploration and use of outer space, including the Moon and other celestial bodies, shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development, and shall be the province of all mankind.*



*Outer space, including the Moon and other celestial bodies, shall be free for exploration and use by all States without discrimination of any kind, on a basis of equality and in accordance with international law, and there shall be free access to all areas of celestial bodies.*

*There shall be freedom of scientific investigation in outer space, including the Moon and other celestial bodies, and States shall facilitate and encourage international cooperation in such investigation.*

These principles provide the reference points for many delegations in COPUOS against which they will judge the relevance and legitimacy of the space sustainability discourse and its outcome.

In addition to the codification of these treaties and principles, progress has also been made in developing a common understanding on other issues related to the exploration and peaceful uses of outer space. All in all, 132 UN General Assembly resolutions or recommendations relating to outer space have been adopted from 1958 to 2018 (UN OOSA 1958–2018). These resolutions have been complemented by additional instruments containing more technically detailed guidance. These instruments include a set of voluntary Space Debris Mitigation Guidelines (UN OOSA 2010) adopted in 2007 and a Safety Framework for Nuclear Power Source Applications in Outer Space, developed jointly by the Scientific and Technical Subcommittee of COPUOS and the International Atomic Energy Agency, which was adopted in 2009 (UN COPUOS and IAEA 2009).

The UN also maintains a Register of Objects Launched into Outer Space that contains information provided by member states and intergovernmental organizations that are party to the Registration Convention (UN Register). As of 1 January 2019, 69 states had acceded to or ratified the Convention, and another four states had signed it. As of 30 August 2019, the Register contained 8737 space objects launched by 87 states or international intergovernmental organizations, for which an international space object designator had been assigned. It is worth noting that only 7859 of those space objects had been registered with the United Nations.

---

## **COPUOS and Space Sustainability**

### **Introduction of the Long-Term Sustainability of Outer Space Activities on the Agenda of COPUOS**

Although several aspects of the work of COPUOS are directly relevant to space sustainability, prior to 2010 these topics were being addressed in isolation; the emergence of a more holistic view of these issues goes back to 2005, as the Committee was approaching its 50th year. In that year, Mr. Karl Deutsch of Canada (Chair of the STSC from 2001 to 2003) presented a discussion paper to the Committee on the future role of COPUOS in its next 50 years. Deutsch made the connection between the sustainability of life on Earth and the cooperative international use of space systems; the very subject COPUOS was established to address.

In 2006–2007, the Committee was chaired by Mr. Gérard Brachet of France. He highlighted the issue of space sustainability during his term as Chairman of COPUOS. At the 50th session of the Committee in 2007, Brachet presented a working paper by the Chair (UN GA 2007) that identified the long-term sustainability of outer space activities as one of the key challenges facing the future peaceful uses of outer space. The working paper further suggested that a working group could be established within the STSC to produce a technical assessment of the situation and to suggest a way forward.

In their sessions during 2008, the STSC and COPUOS discussed the introduction of an agenda item dealing with the long-term sustainability of outer space activities and what such an agenda item might encompass. Subsequently, in 2009, at the 46th session of the STSC, a proposal was put forward by the delegation of France to include a new agenda item on the long-term sustainability of outer space activities on the agenda of the STSC.

At its 52nd session in 2009, COPUOS agreed that the STSC should include, starting from its 47th session in 2010, a new agenda item titled “long-term sustainability of outer space activities” and it proposed a multi-year work plan that was to culminate in a report on the long-term sustainability of outer space activities and a set of best-practice guidelines for presentation to and review by the Committee.

In 2010 the STSC established the Working Group on the Long-Term Sustainability of Outer Space Activities under the chairmanship of Mr. Peter Martinez of South Africa. The first issue to be addressed was reaching agreement on the terms of reference, scope, and methods of work. These deliberations were concluded at the 54th session of COPUOS in June 2011.

This is a very condensed review of the emergence of the long-term space sustainability work in COPUOS. Readers interested in a more detailed review are referred to the article by Brachet (2012).

## **COPUOS Working Group on the Long-Term Sustainability of Outer Space Activities**

The terms of reference for this Working Group (UN GA 2011) mandated it to examine the long-term sustainability of outer space activities in the wider context of sustainable development on Earth, including the contribution of space activities to the achievement of the Millennium Development Goals, taking into account the concerns and interests of all countries. (Nowadays we would refer to the Sustainable Development Goals (SDGs), but the terms of reference for the Working Group predated the adoption of the SDGs at a special UN Summit of Heads of State in September 2015. The SDGs are in a sense the successors of the Millennium Development Goals, and hence the same importance (if not more) is attached to ensuring continuity of space-derived data and services to meet these developmental goals.)

The Working Group was mandated to consider established practices, operating procedures, technical standards, and policies associated with the long-term sustainability of outer space activities throughout all the phases of a mission life cycle. The

Working Group took as its legal framework the existing UN treaties and principles governing the activities of states in the exploration and use of outer space; it did not consider the development of new legally binding instruments.

The Working Group was tasked to produce a report on the long-term sustainability of outer space activities and a consolidated set of voluntary best-practice guidelines that could be applied by states, international organizations, national nongovernmental organizations, and private sector entities to enhance the long-term sustainability of outer space activities for all space actors and for all beneficiaries of space activities.

It is instructive to quote from the terms of reference regarding the expected character of the guidelines to be produced. These guidelines should:

- (a) *Create a framework for possible development and enhancement of national and international practices pertaining to enhancing the long-term sustainability of outer space activities, including, inter alia, the improvement of the safety of space operations and the protection of the space environment, giving consideration to acceptable and reasonable financial and other connotations and taking into account the needs and interests of developing countries.*
- (b) *Be consistent with existing international legal frameworks for outer space activities and should be voluntary and not be legally binding.*
- (c) *Be consistent with the relevant activities and recommendations of the Committee and its Subcommittees, as well as of other working groups thereof, United Nations intergovernmental organizations and bodies and the Inter-Agency Space Debris Coordination Committee and other relevant international organizations, taking into account their status and competence.*

### **Consideration of Topics**

In developing its terms of reference, the Working Group identified a wide range of topics of relevance to the overall considerations of space sustainability, spanning from developmental issues to operational issues, space debris, space weather, and also regulatory issues.

The topics were clustered to allow more efficient consideration of related matters, and four expert groups were established to consider these related sets of topics. These expert groups were populated with experts nominated by their national governments. However, the experts served in an ad hominem capacity and did not necessarily represent their governments' positions in all matters. The expert groups were tasked to contribute inputs to the report of the Working Group and to propose candidate guidelines for consideration by the Working Group. The Working Group was to consider these inputs from the expert groups and take any necessary decisions. In this way, a clear separation was established between the expert groups as technical deliberative fora and the Working Group as a diplomatic negotiating forum.

Based on the inputs from the individual experts and other external inputs (see the subsequent sections titled "[Coordination with Other International Intergovernmental Entities and Processes](#)" and "[Contributions by Non-state Actors](#)"), the expert groups were tasked to identify issues for which sufficient international expert consensus could be found to recommend guidelines based on established best practices. Where the experts identified issues pertinent to the long-term sustainability of outer space

activities, but for which the state of knowledge was such that the experts were not yet able to recommend consensus guidelines based on any operational experience, those issues were referred to the Working Group for its attention and possible future consideration.

The four expert groups and their scopes were as follows:

(a) *Expert Group A: Sustainable space utilization supporting sustainable development on Earth*

Co-chaired by Mr. Filipe Duarte Santos (Portugal) and Mr. Enrique Pacheco Cabrera (Mexico)

This expert group addressed the societal benefits of space activities and their contribution to sustainable development on Earth. It considered space as a shared natural resource, the equitable access to outer space and to the resources and benefits associated with it, as well as access to the benefits of outer space activities for human development. This expert group also considered the role of international cooperation in ensuring that outer space continues to be used for peaceful purposes for the benefit of all nations. This expert group proposed seven candidate guidelines and four topics for further consideration by the Working Group.

(b) *Expert Group B: Space debris, space operations and tools to support collaborative space situational awareness*

Co-chaired by Mr. Richard Buenneke (United States of America) and Mr. Claudio Portelli (Italy)

This expert group considered the issues that make the space environment unpredictable and unsafe for space actors. This included an analysis of risks from space debris and measures to reduce the creation and proliferation of space debris. The implementation of such measures requires strengthened cooperative space situational awareness, which in turn requires the collection, sharing, and dissemination of data on space objects, such as orbits, pre-launch, and pre-maneuver notifications. This expert group also considered tools to support collaborative space situational awareness, such as registries of operators and contact information and procedures for sharing relevant operational information among space actors. This led to a recognition of the importance of developing common standards and practices for information exchange. This expert group proposed eight candidate guidelines and three topics for further consideration by the Working Group.

(c) *Expert Group C: Space weather*

Co-chaired by Mr. Takahiro Obara (Japan) and Mr. Ian Mann (Canada)

This expert group focused on ways to reduce the risks of detrimental effects of space weather phenomena on operational space systems. Such risks may be reduced through the sharing and dissemination of key data on phenomena related to space weather in real or near-real time, as well as sharing of models and forecasts. This expert group proposed five candidate guidelines and two topics for further consideration by the Working Group.

(d) *Expert Group D: Regulatory regimes and guidance for actors*

Co-chaired by Mr. Anthony Wicht (Australia) and Mr. Sergio Marchisio (Italy)

This expert group considered the contribution of international and national legal instruments and regulatory practices to promote the long-term sustainability of outer space activities. This included considerations of how the existing treaties and principles that define the international legal framework for space activities are being implemented at the national level through legal and regulatory regimes and how such national regulatory frameworks for space activities could be developed or further strengthened to support the long-term sustainability of space activities. This expert group proposed eleven candidate guidelines and five topics for further consideration by the Working Group.

The expert groups did not work in silos. Several issues under consideration by the expert groups were intrinsically multidisciplinary in character and therefore fell within the competence of more than one of the expert groups. For this reason, the expert groups held joint meetings to discuss overlaps and gaps.

The expert groups met during the sessions of COPUOS and its STSC from 2011 to 2014 and also took the opportunity of meeting at the International Astronautical Congress in Cape Town in 2011, Naples in 2012, and Beijing in 2013. The four expert groups concluded their work in 2014 and submitted their reports to the Working Group, containing a total of 33 proposed draft guidelines.

### **Coordination with Other International Intergovernmental Entities and Processes**

The Working Group was mandated to liaise with the UN Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities, the Conference on Disarmament, the Commission on Sustainable Development, the International Civil Aviation Organization, the International Telecommunication Union, and the World Meteorological Organization, as well as relevant intergovernmental organizations, such as the European Space Agency, the European Organization for the Exploitation of Meteorological Satellites, the Asia-Pacific Space Cooperation Organization, and the Group on Earth Observations.

The overarching principle behind these interactions was that the Working Group should avoid duplicating the work being done within these international entities while at the same time identifying areas of concern relating to the long-term sustainability of outer space activities that were not being covered by them.

### **Contributions by Non-state Actors**

Although the discussions within the Working Group occurred at the intergovernmental level of COPUOS, states recognized that non-state actors play an important role in the space arena and have much knowledge and experience to contribute to the formulation of guidelines based on the best practices.

A number of international organizations and bodies, such as the Consultative Committee for Space Data Systems, the Inter-Agency Space Debris Coordination

Committee, the International Space Environment Service, the International Organization for Standardization, the International Academy of Astronautics, the International Astronautical Federation, and the Committee on Space Research, also provided inputs into the work of the Working Group and its expert groups.

Commercial operators have extensive experience in running their fleets of spacecraft and in dealing with space weather and other on-orbit operational issues. A case in point was the industry coordination that took place during the Galaxy-15 “zombie sat” episode in 2010 (Weeden 2010). Industry associations and entities such as the International Astronautical Federation provide access to the collective expertise of the space industry and space agencies.

Finally, there are institutional actors focusing on the governance of space activities, such as the European Space Policy Institute or the Secure World Foundation, that analyze certain topics in depth and prepare position papers. These entities also made valuable contributions to the space sustainability dialogue in COPUOS.

The role of non-state actors is at times a contentious issue in COPUOS. Some member states (usually those with a well-established space industry) are comfortable with engaging the private sector in issues on the COPUOS agenda, while others (usually the ones without a space industry) are concerned that the agenda of COPUOS should not be dictated by the interests of commercial entities. Those states are of the view that COPUOS is a forum of states and that states should direct the agenda and discussions in COPUOS.

Because consensus could not be reached on the direct participation of non-state entities in the Working Group, the solution that was agreed upon was to continue with the established practice that states could choose to include in their delegation representatives of their own national non-state entities. In this way, the contributions of experts from non-state entities were made possible. The inputs of national nongovernmental organizations and private sector entities were thus obtained through the member states of COPUOS.

### **Negotiation of the LTS Guidelines**

Following the expert group phase, the Working Group began developing the draft guidelines based on the recommendations of the expert groups. A number of member states also proposed draft guidelines for consideration by the Working Group. By the start of 2016, through a process of consolidation and streamlining, the Working Group had narrowed its focus to 29 draft guidelines, all at various stages of maturity.

From the start of the Working Group in 2010 to the end of its mandate in 2018, the membership of COPUOS grew from 70 to 92 states. Moreover, as the LTS discussions gained momentum in COPUOS, more states became actively engaged in the debates. Since COPUOS takes decisions by absolute consensus of its member states, all member states had to reach agreement on the text of each one of these guidelines, in all six official languages of the UN. Progress was gradual and uneven, but by June 2016 COPUOS reached agreement on the first 12 guidelines (UN COPUOS 2016). In February 2018, at the 55th session of the STSC, agreement was reached on a further nine guidelines and the text of a politically significant context-setting

preamble that included the following definition of space sustainability (UN COPUOS 2018a):

*The long-term sustainability of outer space activities is defined as the ability to maintain the conduct of space activities indefinitely into the future in a manner that realizes the objectives of equitable access to the benefits of the exploration and use of outer space for peaceful purposes, in order to meet the needs of the present generations while preserving the outer space environment for future generations.*

Readers will notice the parallels between this COPUOS definition of space sustainability and the definition of sustainable development mentioned earlier in the section titled “[Space Sustainability](#).”

In addition to the 21 agreed guidelines, there were a further seven draft guidelines (UN COPUOS 2018b) for which the Working Group could not reach consensus during its mandate, which expired in June 2018. Discussions at the 61st session of COPUOS in June 2018 were inconclusive because the Committee could not reach consensus on the way forward and some states could not agree to decoupling the already agreed guidelines from those still under discussion. The session ended in a stalemate, with all states however agreeing that the LTS discussions should continue in 2019.

At its 62nd session in June 2019, the Committee adopted the preamble and 21 guidelines for the long-term sustainability of outer space activities (UN GA 2019). The Committee encouraged states and international intergovernmental organizations to voluntarily take measures to ensure that the guidelines were implemented to the greatest extent feasible and practicable.

The Committee also agreed on the establishment of a new Working Group with a 5-year work plan under the STSC to advance the work on LTS. The Committee decided that this new Working Group would agree on its own terms of reference, methods of work, and dedicated work plan at the 57th session of the STSC, in February 2020. This new Working Group is expected to focus on:

- (a) Identifying and studying challenges for the long-term sustainability of outer space activities and to consider possible new guidelines, including those proposed but not agreed within in the previous Working Group;
- (b) Sharing experiences, practices, and lessons learned from voluntary national implementation of the already adopted guidelines;
- (c) Raising awareness and building capacity to implement the adopted LTS guidelines, in particular among emerging space nations and developing countries.

---

## The Guidelines

The 21 agreed guidelines (UN GA 2019) comprise a collection of internationally recognized measures for ensuring the long-term sustainability of outer space activities and for enhancing the safety of space operations. They address the policy,

regulatory, operational, safety, scientific, technical, and international cooperation and capacity-building aspects of space activities. They are based on a substantial body of knowledge, as well as the experiences of states, international intergovernmental organizations, and relevant national and international nongovernmental entities. Therefore, the guidelines are relevant to both governmental and nongovernmental entities. They are also relevant to all space activities, whether planned or ongoing, as practicable, and to all phases of a space mission, including launch, operation, and end-of-life disposal.

The purpose of the guidelines is to assist states and international intergovernmental organizations, both individually and collectively, to mitigate the risks associated with the conduct of outer space activities so that present benefits can be sustained and future opportunities realized. Consequently, the implementation of the guidelines should promote international cooperation in the peaceful use and exploration of outer space.

These 21 agreed guidelines represent the low-hanging fruit of the LTS discussions, but they also mark a significant step forward in that they represent the tangible progress that has been made in COPUOS in addressing space sustainability. This first set of agreed guidelines creates a foundation for further consensus building in COPUOS.

The guidelines are intended to support the development of national and international practices and safety frameworks for conducting outer space activities while allowing for flexibility in adapting such practices and frameworks to specific national circumstances. They are also intended to support states and international intergovernmental organizations in developing their space capabilities in a manner that avoids causing harm to the outer space environment and the safety of space operations.

The guidelines are voluntary and not legally binding under international law. The existing UN treaties and principles on outer space provide the fundamental legal framework for these guidelines. However, despite their non-binding status under international law, the guidelines can have a legal character in the sense that states may choose to incorporate elements of the guidelines in their national legislation, as has been the case with the COPUOS Space Debris Mitigation Guidelines.

The titles of the 21 agreed guidelines are indicated below. The full text of the guidelines is available in UN document A/74/20, Annex II. The remaining seven draft guidelines that did not reach consensus during the mandate of the Working Group are contained in UN document A/AC.105/C.1/L.367. The progress made in discussions of those draft guidelines will inform future discussions of space sustainability in COPUOS.

#### *A. Policy and regulatory framework for space activities*

Guideline A.1: Adopt, revise and amend, as necessary, national regulatory frameworks for outer space activities

Guideline A.2: Consider a number of elements when developing, revising or amending, as necessary, national regulatory frameworks for outer space activities



- Guideline A.3: Supervise national space activities
- Guideline A.4: Ensure the equitable, rational and efficient use of the radio frequency spectrum and the various orbital regions used by satellites
- Guideline A.5: Enhance the practice of registering space objects
- B. *Safety of space operations*
  - Guideline B.1: Provide updated contact information and share information on space objects and orbital events
  - Guideline B.2: Improve accuracy of orbital data on space objects and enhance the practice and utility of sharing orbital information on space objects
  - Guideline B.3: Promote the collection, sharing and dissemination of space debris monitoring information
  - Guideline B.4: Perform conjunction assessment during all orbital phases of controlled flight
  - Guideline B.5: Develop practical approaches for pre-launch conjunction assessment
  - Guideline B.6: Share operational space weather data and forecasts
  - Guideline B.7: Develop space weather models and tools and collect established practices on the mitigation of space weather effects
  - Guideline B.8: Design and operation of space objects regardless of their physical and operational characteristics
  - Guideline B.9: Take measures to address risks associated with the uncontrolled re-entry of space objects
  - Guideline B.10: Observe measures of precaution when using sources of laser beams passing through outer space
- C. *International cooperation, capacity-building, and awareness*
  - Guideline C.1: Promote and facilitate international cooperation in support of the long-term sustainability of outer space activities
  - Guideline C.2: Share experience related to the long-term sustainability of outer space activities and develop new procedures, as appropriate, for information exchange
  - Guideline C.3: Promote and support capacity-building
  - Guideline C.4: Raise awareness of space activities
- D. *Scientific and technical research and development*
  - Guideline D.1: Promote and support research into and the development of ways to support sustainable exploration and use of outer space
  - Guideline D.2: Investigate and consider new measures to manage the space debris population in the long term

---

## Implementation and Updating of the Guidelines

States and international intergovernmental organizations are encouraged to implement these guidelines to the greatest extent feasible and practicable, in accordance with their respective needs, conditions and capabilities, and with their existing obligations under applicable international law.

International cooperation is required to implement the guidelines effectively and to monitor their impact and effectiveness. However, COPUOS recognizes that not all space actors have equal capability or capacity to implement these guidelines. Therefore, the guidelines place a strong emphasis on international cooperation and information sharing. States and international intergovernmental organizations with extensive experience in conducting space activities are encouraged to support developing countries to strengthen their national capacities to implement the guidelines.

COPUOS also recognizes that these guidelines should be a “living document” that is periodically updated to ensure that, as space activities evolve, the guidelines continue to reflect the most current state of knowledge of pertinent factors influencing the long-term sustainability of outer space activities. This “living document” aspect of the guidelines is especially important given that the rapid evolution in space activities makes space sustainability a dynamic, multi-scale problem.

States and international intergovernmental organizations are encouraged to share their practices and experiences with COPUOS regarding the implementation of the guidelines. States are also encouraged to promote and/or conduct research on topics relevant to these guidelines and their implementation.

COPUOS envisages that it may periodically review, revise, or add to these guidelines to ensure that they continue to provide effective guidance to promote the long-term sustainability of outer space activities. Proposals for revising this set of guidelines, or for new guidelines, may be submitted by any COPUOS member state for consideration by the Committee.

---

## **Other Multilateral Initiatives with a Connection to Space Sustainability**

The COPUOS work on space sustainability did not occur in a vacuum. There were, in fact, several concurrent discussions in other fora that related to space security and space sustainability. Those initiatives were (and some still are) to some extent addressing a set of largely overlapping concerns from the perspectives of different groups of actors and different fora. In this section we briefly consider how the work of COPUOS on space sustainability relates to those other initiatives.

### **Conference on Disarmament**

Given the importance of military and civilian space systems in modern warfare, there is a technical possibility that such systems could be targeted in a conflict situation. The possibility that space-based weapons might be developed and deployed in outer space has given rise to concerns that this could lead to an arms race in outer space. Given that COPUOS focuses exclusively on the peaceful uses of outer space, questions of space weaponization and related security implications are dealt with at the Conference on Disarmament (CD), the sole multilateral body for negotiating arms control issues.

Within the CD, a number of delegations, notably China and Russia, have raised the issue of the Prevention of an Arms Race in Outer Space (PAROS). However, the CD has effectively been stagnant since 1988, since the member states have been unable to agree on the annual program of work. Not only do the members of the CD disagree over its priorities, but also the consensus rule, which served this body well in the past, is now being used to maintain the deadlock. It is against this backdrop that in 2008 China and Russia introduced a Draft Treaty on the Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects (PPWT). However, not all countries agree that new legal instruments to prevent space weaponization are warranted or even beneficial. So, for the time being, the PAROS discussions in the CD are making no progress because of differences of opinion on some fundamental issues. However, there is agreement on the urgency to make progress in those areas where there is consensus, even if such progress must be made outside the CD.

This impasse in the CD had an influence in COPUOS in the sense that the countries supporting the PPWT proposals in the CD did not want the LTS discussions in COPUOS to be used as a pretext to circumvent the need for discussions on the prevention of an arms race in outer space and the development of a legally binding framework to prevent the placement of weapons in outer space. Thus, the terms of reference for the LTS Working Group called for “appropriate liaison” with the CD. The mandate of COPUOS covers only the peaceful uses of outer space, but some of the LTS guidelines could be seen as *de facto* transparency and confidence-building measures to enhance collective space security. In this way the implementation of the COPUOS LTS guidelines could potentially be useful for improving mutual understanding and for reducing misperceptions and mistrust, thereby ultimately promoting a more favorable climate for arms control and nonproliferation discussions in the CD.

### **UN Group of Governmental Experts on Transparency and Confidence-Building Measures (TCBMs) in Outer Space Activities**

In 2010, the UN General Assembly adopted resolution A/Res/65/68 (UN GA 2010), which called for the establishment of a Group of Governmental Experts (GGE) on “Transparency and Confidence-Building Measures in Outer Space Activities.” The GGE was to conduct a study on outer space TCBMs, making use of the relevant reports of the UN Secretary-General, and without prejudice to the substantive discussions on the prevention of an arms race in outer space within the framework of the CD, and to submit to the General Assembly at its 68th session a report with an annex containing the study of governmental experts.

The GGE, which comprised 15 experts selected on the basis of their knowledge and geographical representation, began its work in July 2012 and submitted its final consensus report (document A/RES/65/68) to the First Committee of the UN General Assembly in October 2012. The report was adopted as resolution 68/50 by a unanimous vote in the First Committee and on 10 December 2012 by the General Assembly. This resolution welcoming the GGE report and endorsing its

content was co-sponsored by China, Russia, and the United States and represented a diplomatic breakthrough since the United States had never before voted in favor of the annual TCBM resolution.

The LTS Working Group was tasked in its terms of reference to consider appropriate linkages with the GGE. This was done by the Chairs of two respective processes providing formal briefings to each other's groups. It is instructive to identify some interlinkages between the LTS guidelines and the recommendations contained in the GGE report (UN GA 2010).

The GGE report refers in paragraph 39 to exchanges of information on orbital parameters of outer space objects and potential orbital conjunctions. Reference is also made to the registration of space objects. The LTS guidelines concerning the exchange of contact information, exchange of data on space objects, and risk assessments relating to space objects address such matters.

The GGE report refers in paragraph 40 to exchanges of information on forecast natural hazards in outer space. The LTS guidelines on sharing of operational space weather data, forecasts, and best practices address this issue.

Paragraph 42 of the GGE report refers to notifications relating to scheduled maneuvers that may result in a risk to the flight safety of space objects of other states. The LTS guidelines on the safety of space operations address such matters.

Section V of the GGE report refers to international cooperation and touches, inter alia, on international cooperation for capacity-building and confidence-building. The LTS guidelines on international cooperation in support of long-term sustainability and capacity-building address such issues.

## **The EU Proposal for an International Code of Conduct for Outer Space Activities**

More or less at the same time as the multilateral discussions in COPUOS on the long-term sustainability of outer space activities started, the European Union began a political initiative to develop a Code of Conduct for Outer Space Activities. This initiative was pursued outside of the existing multilateral fora, motivated at least in part as a means to bypass the stalemate on the PAROS issue in the CD and the difficulties posed by the consensus rule in both COPUOS and the CD. The EU expressed its intent to open the code for signature at an international diplomatic conference, to be convened for this purpose.

Outside of Europe, no other major space powers openly endorsed the initiative until January 2012, when US Secretary of State Hillary Clinton announced that "the United States has decided to join with the European Union and other nations to develop an International Code of Conduct for Outer Space Activities" (US Secretary of State 2012). Australia's Foreign Minister, Kevin Rudd, soon followed with a similar statement. However, the initiative was not embraced by a significant number of non-EU space-capable states (notably Brazil, Russia, India, China, and South Africa, the so-called BRICS countries), largely because of concerns about the process and the intent of the EU in having kept this initiative out of multilateral fora. (During the development of the draft code, the EU held numerous bilateral

consultations, but no multilateral consultations in the UN format, until 5 June 2012, when the EU External Action/Information Service held an information session on the margins of COPUOS.) This meant that the Code of Conduct initiative had no formal multilateral mandate, unlike the GGE on space TCBMs and the COPUOS LTS processes. This lack of a formal multilateral mandate ultimately led to the demise of the Code of Conduct initiative, on procedural grounds, at a special meeting held at the United Nations in New York in July 2015.

The failure of the late attempt by the EU to “multilateralize” the code through this special UN meeting had a positive ripple effect on the LTS discussions in the COPUOS. From the start of the LTS discussions in COPUOS, a number of delegations had questioned how the long-term sustainability work related to the EU’s efforts to promote a Code of Conduct and whether such a Code of Conduct would in some way “trump” the long-term sustainability discussions in COPUOS. This had caused a number of delegations to hold back from full engagement in the LTS discussions, waiting to see how the Code discussions were going to play out. With the demise of the Code discussions, COPUOS became the only forum holding productive multilateral space sustainability discussions.

It is worth noting that, although some observers saw the Code of Conduct and LTS discussions as competing processes, a closer examination would show that, although the underlying goals were the same, their approaches were diametrically opposed. The COPUOS LTS work was a technically based, bottom-up approach of developing guidelines based on the collected best practices of established space actors. The Code of Conduct initiative was a more political, top-down approach. The two approaches could, in fact, have complemented each other if the 2015 efforts to multilateralize the Code of Conduct had succeeded.

Since July 2015, the EU has not actively promoted the Code of Conduct, but it has not given up on the idea either. In several statements delivered in multilateral fora in the past 2 years, the EU has expressed the view that it still believes there would be value in agreeing on an instrument that encourages States to make a voluntary political commitment not to undertake activities detrimental to the safety, security, and sustainability of outer space activities. Such a voluntary instrument, potentially to be negotiated within the framework of the UN, should, in the EU’s view, not duplicate the work of COPUOS as the UN’s mandated norm-creating body for the peaceful uses of outer space and should respect its role in the further development of the legal regime governing space activities. Such a voluntary instrument would build upon the COPUOS LTS guidelines and would be complementary to these guidelines. As of this writing (August 2019), it is not yet clear whether or how the EU intends to translate these ideas into diplomatic initiatives.

### **Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space**

For completeness, we will mention here the Group of Governmental Experts on further practical measures for the prevention of an arms race in outer space. This GGE was established pursuant to resolution 72/250, adopted by the General

Assembly on 24 December 2017, and was tasked to “consider and make recommendations on substantial elements of an international legally binding instrument on the prevention of an arms race in outer space, including, inter alia, on the prevention of the placement of weapons in outer space.” This GGE, which comprised experts from 25 nations, carried out its work in 2018 and early 2019 under the leadership of Brazil’s ambassador to the Conference on Disarmament, Guilherme de Aguiar Patriota.

In accordance with its mandate, the GGE considered recommendations on substantial elements of an international legally binding instrument on the prevention of an arms race in outer space, including on the prevention of the placement of weapons in outer space. Pursuant to this mandate, it discussed (a) the international security situation in outer space; (b) the existing legal regime applicable to the prevention of an arms race in outer space; (c) the application of the right to self-defense in outer space; (d) general principles; (e) general obligations; (f) definitions; (g) monitoring, verification, and transparency and confidence-building measures; (h) international cooperation; and (i) final provisions, including institutional arrangements.

The sessions of this GGE took place against a backdrop of elevated political rhetoric around the counterspace developments in recent years, and the Indian anti-satellite (ASAT) test of March 2019 took place during the final session of the GGE, further adding to the grim disarmament climate. The GGE considered several drafts of a substantive report. No consensus was reached on a substantive report, so the GGE’s final report was simply a procedural report issued as UN document A/74/77. Although this outcome was disappointing, the process itself was important in that the GGE held substantive discussions on space arms control.

---

## Concluding Remarks

The golden thread running through the processes in COPUOS, the GGE on space TCBMs, and the Code of Conduct initiative is that they were all aiming to produce instruments that are voluntary in nature. However, although such instruments may be legally non-binding, they are politically binding. Another important point to appreciate is that *non-binding* does not mean *non-legal*, in the sense that states can choose to domesticate their politically binding agreement to such voluntary frameworks in their domestic regulatory practices.

A number of countries have expressed concern that such voluntary instruments are inherently fragile and would not prove effective in preventing the weaponization of and an arms race in outer space. However, there does not seem to be consensus at this point on the desirability of legally binding instruments banning the placement and use of weapons in outer space, so the development of voluntary frameworks for promoting space sustainability provides some scope for making progress. Voluntary frameworks do not necessarily retard the evolution of binding norms and can in fact pave the way for adoption of binding norms. Historically, many legal rules have resulted from the codification of existing practices adopted by consensus.

Progress will also be made in the sense that the states that choose to participate in these processes do so because they recognize the urgency of addressing the problems of space sustainability and space security. That awareness in and of itself may be enough to convince space actors to take corrective and preventative actions on their own. The COPUOS LTS guidelines, while non-binding, have the advantage of being the result of a multilateral consensus-based process and will therefore have a good chance of being implemented by space actors, in their own interest.

---

## References

- Brachet G (2012) The origins of the long-term sustainability of outer space activities initiative at UN COPUOS. *Space Policy* 28:161–165
- Hedman N, Balogh W (2009) The United Nations and outer space: celebrating 50 years of space achievements. In: Schrogl K-U, Mathieu C, Peter N (eds) *Yearbook on Space Policy 2007/2008: from policies to programmes*. Springer, Wien/New York, pp 237–250. ISBN: 978-3-211-99090-2
- Outer Space Treaty (1967) The treaty on principles governing the activities of States in the exploration and use of outer space, including the moon and other celestial bodies, of 27 January 1967. <http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html>. Accessed 3 Feb 2020
- United Nations Committee on the Peaceful Uses of Outer Space (2016) Report of the fifty-ninth session, The first batch of agreed guidelines is contained in the Annex to the report of the 59th session of COPUOS in 2016, contained in UN document A/71/20. [http://www.unoosa.org/oosa/oosadoc/data/documents/2016/a/a7120\\_0.html](http://www.unoosa.org/oosa/oosadoc/data/documents/2016/a/a7120_0.html). Accessed 3 Feb 2020
- United Nations Committee on the Peaceful Uses of Outer Space (2018a) Working Group on the Long-Term Sustainability of Outer Space Activities: preambular text and nine guidelines, conference room paper by the Chair of the Working Group on the Long-Term Sustainability of Outer Space Activities. UN document A/AC.105/C.1/2018/CRP.18/Rev.1. [http://www.unoosa.org/res/oosadoc/data/documents/2018/aac\\_105c\\_1201\\_8crp/aac\\_105c\\_12018crp\\_18rev\\_1\\_0\\_html/AC105\\_C1\\_2018\\_CRP18Rev01E.pdf](http://www.unoosa.org/res/oosadoc/data/documents/2018/aac_105c_1201_8crp/aac_105c_12018crp_18rev_1_0_html/AC105_C1_2018_CRP18Rev01E.pdf). Accessed 3 Feb 2020
- United Nations Committee on the Peaceful Uses of Outer Space (2018b) Draft guidelines for the long-term sustainability of outer space activities, working paper by the Chair of the Working Group on the Long-Term Sustainability of Outer Space Activities. The most mature expression of these draft guidelines is contained in UN document A/AC.105/C.1/L.367. [http://www.unoosa.org/res/oosadoc/data/documents/2019/aac\\_105c\\_11/aac\\_105c\\_11\\_367\\_0\\_html/V1804974.pdf](http://www.unoosa.org/res/oosadoc/data/documents/2019/aac_105c_11/aac_105c_11_367_0_html/V1804974.pdf). Accessed 3 Feb 2020
- United Nations Committee on the Peaceful Uses of Outer Space Scientific and Technical Subcommittee and International Atomic Energy Agency (2009) Safety framework for nuclear power source applications in outer space. International Atomic Energy Agency, Vienna. [www.unoosa.org/pdf/publications/iaea-nps-sfrmwrkE.pdf](http://www.unoosa.org/pdf/publications/iaea-nps-sfrmwrkE.pdf). Accessed 3 Feb 2020
- United Nations General Assembly (1987) Report of the World Commission on Environment and Development, Annex Our Common Future, UN document A/42/427. <http://www.un-documents.net/wced-ocf.htm>. Accessed 3 Feb 2020
- United Nations General Assembly (2007) Committee on the Peaceful Uses of Outer Space, future role and activities of the Committee on the Peaceful Uses of Outer Space, working paper submitted by the Chairman, UN document A/AC.105/L.268. [http://www.unoosa.org/pdf/limited/I/AC105\\_L268E.pdf](http://www.unoosa.org/pdf/limited/I/AC105_L268E.pdf) with a corrigendum issued in document [http://www.unoosa.org/pdf/limited/I/AC105\\_L268Corr1E.pdf](http://www.unoosa.org/pdf/limited/I/AC105_L268Corr1E.pdf). Accessed 3 Feb 2020
- United Nations General Assembly (2010) Resolution adopted by the General Assembly on 8 December 2010, on the report of the First Committee (A/65/410), transparency and

- confidence-building measures in outer space activities, A/RES/65/68. <https://undocs.org/en/A/RES/65/68>. Accessed 3 Feb 2020
- United Nations General Assembly (2011) Report of the Committee on the Peaceful Uses of Outer Space, fifty-fourth session (1–10 June 2011), UN General Assembly document A/66/20, Annex II
- United Nations General Assembly (2019) Report of the Committee on the Peaceful Uses of Outer Space, sixty-second session (12–21 June 2019), the final combined texts of the preamble and 21 LTS guidelines is contained in UN document A/74/20, Annex II. [https://www.unoosa.org/res/oosadoc/data/documents/2019/a/a7420\\_0\\_html/V1906077.pdf](https://www.unoosa.org/res/oosadoc/data/documents/2019/a/a7420_0_html/V1906077.pdf). Accessed 3 Feb 2020
- United Nations Office for Outer Space Affairs (1958–2018) Documents and resolutions database. [www.unoosa.org/pdf/publications/st\\_space\\_49E.pdf](http://www.unoosa.org/pdf/publications/st_space_49E.pdf). Accessed 3 Feb 2020
- United Nations Office for Outer Space Affairs (2010) Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space. United Nations, Vienna. [https://www.unoosa.org/oosa/documents-and-resolutions/search.jsp?lf\\_id=](https://www.unoosa.org/oosa/documents-and-resolutions/search.jsp?lf_id=). Accessed 3 Feb 2020
- United Nations Register of Objects Launched into Outer Space. <http://www.unoosa.org/oosa/en/spaceobjectregister/index.html>. Accessed 3 Feb 2020
- United States Secretary of State (2012) Statement of Hillary Rodham Clinton on January 17, 2012. <http://www.state.gov/secretary/rm/2012/01/180969.htm>. Accessed 3 Feb 2020
- Weeden B (2010) Dealing with Galaxy 15: Zombiesats and on-orbit servicing. *The Space Review*, Edition of 24 May 2010. <http://thespacereview.com/article/1634/1>. Accessed 3 Feb 2020





# Security Issues with Respect to Celestial Bodies

# 18

George D. Kyriakopoulos

## Contents

Introduction .....	342
Celestial Bodies: The Current Status Quo .....	344
Freedom of Exploration and Use; Freedom of Access; Freedom of Scientific Investigation; Non-appropriation .....	344
Applicability of International Law .....	344
Use “Exclusively for Peaceful Purposes” .....	344
Harmful Contamination Is Prohibited .....	345
Right to Visit Facilities and Equipment of Other States .....	345
Threats Arising from the Weaponization of Outer Space .....	345
Prevention of an Arms Race in Outer Space .....	346
Transparency and Confidence-Building Measures in Outer Space Activities (TCBMs) ...	347
Threats Associated with the Evolution of Space Activities on Celestial Bodies: The Space Resources Exploitation Issue .....	348
Extraction and Appropriation of Space Resources: Security Issues .....	349
Applicable International Law .....	350
National Approaches to Space Resource Utilization .....	350
The Resources’ Issue Inside the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) .....	352
The Hague International Space Resources Governance Working Group .....	353
Conclusion .....	354
References .....	355

## Abstract

Space security is part of the overall international security, the maintenance of which constitutes the fundamental purpose of the UN Charter. In particular, preserving security with respect to the celestial bodies requires the activation of mechanisms able to guarantee that the existing *status quo* (global commons’

---

G. D. Kyriakopoulos (✉)  
School of Law, National and Kapodistrian University of Athens, Athens, Greece  
e-mail: [yokygr@gmail.com](mailto:yokygr@gmail.com)

character, applicability of international law, peaceful use, prohibition of harmful contamination) will not be compromised by the placement of offensive weapons on them or potential disputes concerning the exploitation of space resources. Another concern is the control of cosmic hazards (planetary defense), although, in this case, security on Earth will be at stake.

---

## Introduction

Security in international relations is a value. As such, it refers to the maintenance and protection of an international *status quo* against potential threats that would be able to disrupt the current state of affairs (Jakhu and Pelton 2017: 269). At global level, the fundamental regulatory scheme for the protection of post-World War II international society is contained in the Charter of the United Nations, the main purpose of which is “the maintenance of international peace and security” (UN Charter, Preamble). In this respect, Article 1 of the Charter, in listing the purposes of the Organization, refers in particular to the need “to maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace. . . .” Further, it is not by chance that Article 2 paragraph 3 of the Charter provides, among the fundamental principles of the United Nations, that “all Members shall settle their international disputes by peaceful means in such a manner that international peace and security, and justice, are not endangered.”

Given the global character of international security, it is obvious that any threats against it will come from internal actors, such as states or other entities (e.g., terrorist groups). In most cases, these threats will be of an aggressive character. As it was rightly pointed out:

International security is. . . an internal problem for international society as a whole. In this context, the use of armed force is directed at what may in essence be thought as the problem of internal subversion by those who would threaten the plural and cooperative character of international society. Secession, irredentism, aggressive war, conquest, illegal occupation, mass expulsion, genocide and other actions which violate international law all threaten to disrupt the general condition of peace, order and lawfulness within international society. . . . (Jackson-Preece 2011: 20)

Space security is construed in the same way. State relations in the space domain are part of the general scheme of international relations and, in many instances, are able to affect state policies on Earth. The fact that space security should be faced in the context of the fundamental obligation “to maintain international peace and security” is clearly demonstrated in Article III of the *Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies* of 1967 (hereinafter “The Outer Space Treaty” or “OST”), which calls for the applicability, in outer space, of international law, “including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding.”

Outer space constitutes a relatively new field of activity for states that started when the first artificial satellite, Sputnik-1, was launched and put into orbit on 4 October 1957 by the Soviet Union. This achievement was just a first step in the so-called Race to the Moon between the two superpowers of that time, the US and USSR. It is therefore hardly surprising that international space law (which was mainly formed in the 50s, the 60s, and the 70s) reflected in essence the international relations of the Cold War Era and the confrontation of the two space-faring powers of this era. It is thus obvious that, in those days, space security was a game for two. However, the security concerns of the two superpowers finally resulted in an optimal balance, which was reflected in a set of fundamental principles initially formed in the context of Resolution 1962 (XVIII)/1963 of the UN General Assembly and finally incorporated in the Outer Space Treaty.

However, things are changing, and the state of space affairs is now substantially different than in the past. New space actors, mainly coming from the private sector, emerge, intending to operate in “exotic” space activities such as the extraction of asteroid mineral resources or the provision of “space tourism” services.

In view of the above, space security is dependent on the establishment of a regime capable of confronting potential threats “to the advantages that accrue for humanity from the use of space” (Jakhu and Pelton 2017: 269). The purpose of this book is to assess the multiple threats that might compromise space security in toto; however, the object of this particular chapter is to shed light on those aspects of space security that are related to the celestial bodies.

Although the space treaties repeatedly refer to “the exploration and use of outer space, including the Moon and other celestial bodies,” the term “celestial body” is not clearly defined. According to a generic definition, the celestial bodies constitute natural objects “located outside of Earth’s atmosphere, such as the Moon, the Sun, an asteroid, planet, or star.” (<https://www.yourdictionary.com/celestial-body>) Although several theories on the definition of the celestial bodies have emerged, some of them arguing that comets and asteroids cannot be considered as celestial bodies (Pop 2001), there is still no generally accepted definition – at least in the context of the *corpus juris spatialis*. However, it can be argued that the celestial bodies are distinguished from space objects, which are artificial manmade objects (Hobe 2009). For the purposes of this chapter, the celestial bodies are regarded as described in article 1 of the 1979 Moon Agreement: The Moon and “other celestial bodies within the solar system, other than the Earth.”

As stated, security is compromised by internal actors. This means that natural threats to the celestial bodies will not be dealt with in this chapter. Besides, the planetary defense issue (how to address the threat that asteroids and comets represent) is a particular problem for Earth. The presentation below will therefore focus on the situation of celestial bodies as it stands at present, in conformity with the applicable international legal framework, before examining the main causes of potential friction: the possible placement of weapons in outer space (and on celestial bodies) as well as the growing desire for the appropriation of space resources.

## **Celestial Bodies: The Current Status Quo**

According to the legal framework in force, the current status quo of the celestial bodies exhibits some particular characteristics, which are specified below (global commons' regime, applicability of international law, peaceful use, avoidance of harmful contamination). The maintenance of this status quo is a crucial factor in order to preserve security, as far as state activities related to the celestial bodies are concerned. However, in view of the fundamental changes that take place in space affairs, it is possible that a new balance point will be needed in the near future.

## **Freedom of Exploration and Use; Freedom of Access; Freedom of Scientific Investigation; Non-appropriation**

The exploration and use of the celestial bodies shall be carried out for the benefit and in the interests of all countries (it constitutes a "province of all mankind"). All states, "without discrimination of any kind, on a basis of equality and in accordance with international law," are free to explore and use the celestial bodies; further they can freely access all areas of them and, last but not least, they enjoy the freedom of scientific investigation (Article I, Outer Space Treaty, Articles 4 & 6, Moon Agreement).

Moreover, according to the space treaties, the celestial bodies are "not subject to national appropriation by claim of sovereignty, by means of use or occupation, or by any other means" (Article II, Outer Space Treaty), which means that they belong to the so-called "global commons" (spaces beyond national jurisdiction) (Ranganathan 2016: 693, UN System task team on the post-2015 UN Development Agenda 2013: 5). In view of this particular character of the celestial bodies, activities on them "must be conducted with due regard to the corresponding interests of all other States" (Article IX, Outer Space Treaty).

## **Applicability of International Law**

Activities on the celestial bodies must take place "in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding" (Article III, Outer Space Treaty, Article 2, Moon Agreement). In view of the applicability of the UN Charter in space affairs, fundamental precepts of international law, such as the prohibition of the use of force in international relations (Article 2 para. 4) or the "inherent" right to self-defense (Article 51) equally apply to the activities of States in outer space.

## **Use "Exclusively for Peaceful Purposes"**

It is prohibited to States (parties to the Outer Space Treaty) to install nuclear weapons or any other kinds of weapons of mass destruction on celestial bodies (Article IV

para. 1, Outer Space Treaty, Article 3 Moon Agreement). Further, the celestial bodies shall be used “exclusively for peaceful purposes.” In this respect, the establishment of military bases, installations, and fortifications; the testing of any type of weapons; and the conduct of military maneuvers on celestial bodies are forbidden. States are entitled to use equipment or facilities “necessary for peaceful exploration of the Moon and other celestial bodies” (Article IV para. 2, Outer Space Treaty, Article 3 paras. 1–2-4, Moon Agreement). According to the prevailing interpretation, based on state practice, “peaceful” means “non-aggressive” (Tronchetti 2015: 338–340).

### **Harmful Contamination Is Prohibited**

Exploration of the celestial bodies must take place “so as to avoid their harmful contamination and also adverse changes in the environment of the Earth resulting from the introduction of extra-terrestrial matter.” In case of activities, on the celestial bodies, which may cause “potentially harmful interference with activities of other States,” “appropriate international consultations” must be undertaken (Article IX, Outer Space Treaty, Articles 7, 8 para. 3, Moon Agreement).

### **Right to Visit Facilities and Equipment of Other States**

A right of states to visit “all stations, installations, equipment and space vehicles on the Moon and other celestial bodies. . . on a basis of reciprocity,” after “reasonable advance notice” is established in the Outer Space Treaty. Said right must be exercised in such a way as to “assure safety and to avoid interference with normal operations in the facility to be visited” (Article XII).

---

### **Threats Arising from the Weaponization of Outer Space**

Although it is prohibited to use the celestial bodies for non-peaceful purposes (Outer Space Treaty, Article IV para. 2), the issue is far from resolved. It is true that, up to now, those states (US, Russia, China) that possess the technical infrastructure and means to undertake military activities on the celestial bodies (for the time being, on the Moon) have avoided placing weapons in outer space (Schrogl and Neumann 2009: 87; Space Security Index 2019: 97, 132, 137). However, the current legal framework does not prevent states from placing conventional weapons in space and relevant scenarios have been developed in military circles. Thus, the general debate on the weaponization of outer space is still topical.

However, it must be stressed that military activities in outer space that would be permissible under space law must also be compliant with Article 2 para. 4 of the UN Charter. In other words, they must be of a non-aggressive character (Petras 2002: 1255). Furthermore, the “inherent” right to self-defense, pursuant to the UN Charter and the international customary law, is also valid in outer space activities,

notwithstanding the limitations established by Art. IV of the Outer Space Treaty (in the context of the “peaceful purposes”).

Military applications of non-offensive character became common since the beginning of the Space Age, through the use of reconnaissance and early warning satellites. However, the term “weaponization of outer space” refers to the placement of offensive weapons in outer space, encompassing also the development of weapon systems on Earth whose mission is to destroy space objects (Tronchetti 2015: 333–334, Mosteshar 2019). Anti-satellite (ASAT) weapons stand as an example of the latter: they have already been used to destroy satellites in orbit, for testing purposes (Kyriakopoulos 2015: 599). Further, according to existing scenarios, space devices can be used in order to destroy targets on Earth (e.g., use of space for missile interception – Space Security Index 2019: 132), while in addition cyberattacks against satellites is a matter of concern. The situation is made yet more complex by the “dual-use” nature (civil/military) of most space systems (Lyall and Larsen 2018: 448).

## Prevention of an Arms Race in Outer Space

This item was in the Agenda of the Conference on Disarmament (CD) since the early 80s. In 1985, CD mandated a committee especially set up for this purpose to identify and examine issues relevant to the prevention of an arms race in outer space (PAROS), such as the legal protection of satellites, nuclear power systems in space, and various confidence-building measures. It is worth noting that the United States clearly opposed to the mandate of the committee, opting for direct talks with the Soviet Union.

In 2008, China and Russia jointly introduced to the Conference on Disarmament (CD) a draft convention on the prevention of the installation of weapons systems in outer space. The draft treaty, while it recognized that “prevention of the placement of weapons in outer space and of an arms race in outer space would avert a grave danger for international peace and security,” proposed a broad definition of “weapons placed in outer space” by comprising in its scope any such weapon that “orbits the Earth at least once, or follows a section of such an orbit before leaving this orbit, or *is permanently located somewhere in outer space.*” It is thus obvious that weapons that could have been placed on the celestial bodies were brought within the field of application of the draft treaty. This approach was further confirmed in the wording of Article II of the draft, pursuant which states undertook “not to place in orbit around the Earth any objects carrying any kinds of weapons, *not to install such weapons on celestial bodies.* . . .”

On 10 June 2014, Russia submitted to the CD an updated draft of this Convention (Draft Treaty on the Prevention of the Placement of Weapons in Space, the Threat or Use of Force Against Space Objects, PPWT). This revised draft further established the obligation for states “Not to resort to the threat or use of force against outer space objects” of other states (Article II). Such objects can be, *inter alia*, “permanently located . . . on any celestial bodies other than the Earth” (Article I).

Through recurring resolutions, the General Assembly, recognizing the importance of the Transparency and Confidence-Building Measures (TCBMs), has consistently urged the states members to “contribute actively to the objective of the peaceful use of outer space and of the prevention of an arms race in outer space” (A/RES/74/32, 12.12.2019).

### **Transparency and Confidence-Building Measures in Outer Space Activities (TCBMs)**

In 1990, the General Assembly requested the Secretary-General, with the assistance of a group of governmental experts, to carry out a study on different confidence-building measures in outer space. That group delivered its report in 1993 (A/48/305) (Takaya-Umehara 2010: 1301).

In 2011, the UN General Assembly further asked the Secretary-General to set up a “Group of Government Experts” (GGE) to conduct a TCBM survey (A/RES/65/68). The GGE submitted its Report to the Assembly on 29.7.2013 (A/RES/68/189). In this Report, the GGE proposed a set of TCBMs in outer space, including the proposal to establish coordination between United Nations Office for Disarmament Affairs (UNODA), United Nations Office for Outer Space Affairs (UNOOSA), and other appropriate UN entities. Among the measures proposed, the following could be of particular importance with respect to the subject matter of this chapter:

- Exchanges of information on the principles and goals of a State’s outer space policy
- Exchanges of information on major military outer space expenditure and other national security space activities
- Exchanges of information on forecast natural hazards in outer space
- Voluntary familiarization visits
- Expert visits, including visits to space launch sites, invitation of international observers to launch sites, flight command and control centers, and other operations facilities of outer space infrastructure
- International cooperation
- Consultative mechanisms
- Outreach measures
- Measures of coordination

The General Assembly further encouraged the implementation of the TCBMs. On 5 December 2013, with Resolution 68/50, after having reaffirmed that “preventing an arms race in outer space is in the interest of maintaining international peace and security and is an essential condition for the promotion and strengthening of international cooperation in the exploration and use of outer space for peaceful purposes,” the Assembly encouraged Member States to review and implement, “to the greatest extent practicable,” the proposed TCBMs, “through relevant national mechanisms, on a voluntary basis and in a manner consistent with the national interests of Member States.”

Of course, said measures are nonlegally binding voluntary measures. Nevertheless, as it was stated in the GGE Report, “such measures can augment the safety, sustainability and security of day-to-day space operations and can contribute both to the development of mutual understanding and to the strengthening of friendly relations between States and peoples.” Further, the importance of the said TCBMs for the maintenance of space security (and, in particular, for preserving security with respect to celestial bodies) is explicitly recognized in the Report, in its paragraph 31: “In general terms, transparency and confidence-building measures for outer space activities should be aimed at increasing the security, safety and sustainability of outer space. Particular attention should be given to the development and implementation of voluntary and pragmatic measures to ensure the security and stability of all aspects of outer space activities.”

In 2017, a new GGE (“on further practical measures for the prevention of an arms race in outer space”) was established pursuant UNGA Resolution 72/250 (24.12.2017), in order to “consider and make recommendations on substantial elements of an international legally binding instrument on the prevention of an arms race in outer space, including, inter alia, on the prevention of the placement of weapons in outer space.” The Group met in two sessions, the first from 6 to 17 August 2018 and the second from 18 to 29 March 2019. However, no consensus was reached on a substantive report (A/74/77, Note by the Secretary-General).

Following the aforementioned resolutions of the General Assembly, a European Union initiative took the form of a Draft International Code of Conduct for Outer Space Activities. Having noted, in its preamble, the importance of preventing an arms race in outer space, said code also proposed TCBMs, in order to “prevent confrontation and foster national, regional and global security and stability.” General Principle 28 of the Code emphasized “the responsibility of States, in the conduct of scientific, civil, commercial and military activities, to promote the peaceful exploration and use of outer space for the benefit, and in the interest, of humankind and to take all appropriate measures to prevent outer space from becoming an arena of conflict.”

---

## **Threats Associated with the Evolution of Space Activities on Celestial Bodies: The Space Resources Exploitation Issue**

Over the last few years, there has been a great deal of talk about the development of activities related to the exploration, exploitation, and utilization of outer space resources. This is a space activity for the future, as it requires the development of relevant technology as well as the mobilization of significant financial resources in order for such a challenging adventure to be able to have a sustainable future. Moreover, important security issues are raised.

In the aforementioned context, new space actors emerge, mainly coming from the private sector and intending to operate in areas that a few years ago would be classified as “exotic.”



It is generally accepted that the term “space resource utilization” encompasses activities into Earth orbits, in situ resource utilization (ISRU), as well as the commercial appropriation of space natural resources (“space mining”). Earth orbits are outside the thematic area of this chapter. ISRU is the collection, processing, storing, and use of materials encountered in the course of human or robotic space exploration that replace materials that would otherwise be brought from Earth to accomplish a mission’s critical need at reduced overall cost and risk (Sackstender and Sanders 2007). ISRU, provided it is compatible with article IX OST, constitutes an activity that is in conformity with article I paragraphs 2 and 3 of the Outer Space Treaty, as it is associated with the freedom of use, exploration, and scientific investigation of outer space and, in principle, does not constitute appropriation. However, in due time an ad hoc regulation of ISRU could help to avoid tensions, if such use is to take place by numerous users in a common area on a celestial body. Thus, it is the commercial exploitation of space resources that will be discussed in further detail.

### **Extraction and Appropriation of Space Resources: Security Issues**

The National Aeronautics and Space Administration (NASA) claims that there are approximately 100,000 near-Earth objects, and a great number of them potentially contain water and important minerals, such as nickel, cobalt, and iron. However, is “space mining” feasible, with today’s standards?

On 6 August 2014, ESA’s orbiter “Rosetta” arrived at Comet 67P/Churyumov-Gerasimenko and the lander “Philae” landed on the comet on 12 November 2014. On 8 September 2016, NASA launched OSIRIS-REx, in order to reach the asteroid Bennu and return samples in 2023 (<https://www.nasa.gov/osiris-rex>). These experimental missions clearly pave the way for the commercial exploitation of celestial bodies (comets, asteroids, planets) in the near future.

During the Cold War, the competition of US and USSR for the “conquest of outer space” resulted in a set of fundamental principles, first enshrined in UNGA Resolution 1962 (XVIII) of 13 December 1963 and again in the Outer Space Treaty of 1967. In this context, the balance over potential claims for the existing “wealth” in outer space led to the adoption of the non-appropriation principle. At that time, of course, the technology available did not allow for the exploitation of space resources. However, the situation is now changing drastically, and it is quite possible that in the near future there will be intense competition among states for the appropriation of space resources. It is therefore obvious that, in this area of activity, international security must be strengthened. This obviously requires a global space resources management regime, since any unilateral actions are likely to cause friction between the states concerned. Such a regime should take into account the existing fundamental principles of international space law, given that states do not contest their acceptance.

## Applicable International Law

With respect to the exploration and exploitation of outer space, the *lex lata* provisions are Article I, II, and III of the Outer Space Treaty. Article I provides for the freedom of exploration and use of outer space, including the Moon and other celestial bodies, and for the freedom of access to all areas of celestial bodies. Article II further establishes the non-appropriation principle while, pursuant Article III, activities in the exploration and use of outer space, including the Moon and the celestial bodies, shall be carried on “in accordance with international law, including the Charter of the United Nations, in the interest of maintaining international peace and security and promoting international cooperation and understanding.”

As has been said, there is no specific, ad hoc legal framework for the administration of the space resources exploration, exploitation, and utilization. Nevertheless, the Moon Agreement, although poorly ratified, establishes such a regime, as laid down in Article 11:

1. The Moon and its natural resources are the common heritage of mankind, which finds its expression in the provisions of this Agreement, in particular in paragraph 5 of this article.
2. The Moon is not subject to national appropriation by any claim of sovereignty, by means of use or occupation, or by any other means.
3. Neither the surface nor the subsurface of the Moon, nor any part thereof or natural resources in place, shall become property of any State, international intergovernmental or non-governmental organization, national organization or non-governmental entity or of any natural person. . .
- . . . . .
5. States Parties to this Agreement hereby undertake to establish an international regime, including appropriate procedures, to govern the exploitation of the natural resources of the Moon as such exploitation is about to become feasible. This provision shall be implemented in accordance with article 18 of this Agreement.

However, it is obvious that, for the majority of States that have not yet ratified said instrument, the international norms applicable to the exploration and exploitation of outer space are the aforementioned provisions of the Outer Space Treaty of 1967. It therefore follows that the fundamental principles of international space law in force rather advocate a collective exploitation regime of the resources on the Moon and other celestial bodies, at least in principle.

## National Approaches to Space Resource Utilization

*United States:* In the United States, the commercialization of outer space was encouraged by the *U.S. Commercial Space Launch Act* of 1984, according to which “the general welfare of the United States requires that the Administration

seek and encourage, to the maximum extent possible, the fullest commercial use of space.” At that time, the Act faced only unmanned launch activities, as there was still no question about human space flight. Further, the Act also directed the Federal Aviation Administration (FAA) (through delegations) to encourage, facilitate, and promote commercial space launches and reentries by the private sector, including those involving space flight participants (§ 50903).

On 25 November 2015, the President of the United States signed the *U.S. Commercial Space Launch Competitiveness Act* (H.R. 2262). As far as space mining is concerned, the important part of said Act is its Title IV “Space Resource Exploration and Utilization.” According to this part, emphasis is made to the promotion of the right of U.S. citizens “to engage in commercial exploration for and commercial recovery of space resources free from harmful interference, in accordance with such obligations and subject to authorization and continuing supervision by the federal government.” Furthermore, “A U.S. citizen engaged in commercial recovery of an asteroid resource or a space resource *shall be entitled to any asteroid resource or space resource obtained, including to possess, own, transport, use, and sell it according to applicable law, including U.S. international obligations.*”

It follows that under said Act (in other words, by a unilateral act), U.S. citizens are explicitly entitled, inter alia, to “possess,” “own,” and “sell” asteroid resources; thus the Act explicitly confers to U.S. citizens property rights to resources in outer space, which is in sharp contrast with the principle of non-appropriation enshrined in article II OST.

In the light of this Act, some experts have advanced arguments in favor of the permissibility of space resource utilization/appropriation. However, the prevailing view on the exact meaning of Article II is that the non-appropriation principle prohibits both the exercise of sovereign rights (by states) and private appropriation (by nongovernmental entities) (Freeland and Jakhu 2009: 50). This conclusion is further strengthened by the clear wording of Article 11 paragraph 3 of the Moon Agreement, according to which “Neither the surface nor the subsurface of the Moon, nor any part thereof or natural resources in place, shall become property of any State, international intergovernmental or non-governmental organization, *national organization or non-governmental entity or of any natural person.*”

In this respect, it is worth mentioning that the question of private property claims in outer space has arisen before U.S. courts in the past, when an individual (Gregory Nemitz) claimed parking fees from NASA regarding use of his own asteroid (!). However, the claim was dismissed on the grounds that the Outer Space Treaty did not permit appropriation of private property. In addition, both NASA and the U.S. State Department rejected the claim, thus adopting a broad interpretation of the non-appropriation principle.

*Luxembourg:* Luxembourg adopted a law on the exploration of space and the use of space resources in 2017 (*Loi du 20 juillet 2017 sur l’exploration et l’utilisation des ressources de l’espace*). Article 1 of said law states that “space resources are capable of being appropriated,” which means that extraction companies will have ownership on the space resources that they extract. Further, pursuant Articles 2–4, Luxembourg corporations or European companies that have their registered office

in Luxembourg may extract space resources for commercial use after obtaining approval from the Government of Luxembourg. Again the compatibility of these provisions with the non-appropriation principle is highly questionable.

### **The Resources' Issue Inside the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS)**

Since 2017, the Legal Subcommittee of UNCOPUOS (LSC) has included, as an item in its agenda, a "General exchange of views on potential legal models for activities in the exploration, exploitation and utilization of space resources."

The discussions inside the LSC as well as the practice of states have shown that, at present, there is no consensus among states on the legal regime that should govern the resources issue.

During the 58th session of the LSC (2019), Belgium and Greece submitted a common proposal/working paper (A/AC.105/C.2/L.311/4.3.2019), entitled "Proposal for the establishment of a working group for the development of an international regime for the utilization and exploitation of space resources - Working paper by Belgium and Greece." Said document highlighted the principles of international space law which should govern the future exploitation of the resources of the celestial bodies, in particular:

- That the exploration and use of outer space is a field for all of Humankind
- That such exploration and use is regulated by international law
- That the space treaties require an enhanced international cooperation

As for the impact of the resources' issue on the maintenance of international security on celestial bodies, the working paper mentioned the following (paragraph 16):

The need for an international legal regime for space resource exploitation also arises from the fact that national approaches to space resource exploitation are bound to result in conflicts between competing players, if left to evolve on their own without international guidance. Hence, even if there is no legal objection to States interpreting at will their international obligations under the Outer Space Treaty when regulating space resources, there is still a clear need for an international institutional framework to regulate competing activities. In order for such a framework to be effective, it would have to be focused on the main purposes described in article 11, paragraph 7, of the Moon Agreement, the value of which is greater and goes beyond any views on the ratification of the Moon Agreement. Those purposes include the following: (a) the orderly and safe development of natural resources from outer space; (b) the rational management of those resources; (c) the expansion of opportunities in the use of those resources; and (d) an equitable sharing by all States in the benefits derived from those resources, whereby the interests and needs of the developing countries, as well as the efforts of those countries which have contributed either directly or indirectly to the exploration of outer space, shall be given special consideration.

Based on these principles, the working paper proposed the creation of an ad hoc working group within the framework of the LSC, having as mandate to investigate

the aspects and questions raised with respect to the future use and exploitation of space resources, as well as the preparation of a report. Nevertheless, said proposal did not reach consensus inside the Legal Subcommittee. Instead, the LSC adopted a compromise proposal by the Chair, according to which scheduled informal consultations were to be held at the next session of the Subcommittee, in 2020.

During the 62th session of the COPUOS (2019), a relevant proposal was submitted by the United Arab Emirates (A/AC.105/2019/CRP.17/19.6.2019). The proposal recognized “the importance of establishing a working group that serve as a platform to create a unified strategic conversation among Member States” and considered that said working group “will lead the discussions towards the development of a recommended set of principles governing Space Resources Utilization activities.”

### **The Hague International Space Resources Governance Working Group**

Beyond the discussions that take place in the context of the COPUOS, The Hague International Space Resources Governance Working Group is another forum that examined the space resources’ issue. The Working Group was established in 2016, in order to assess the need for a governance framework on space resources, and consists of members as well as observers that represent governments as well as industry, academia, science, international organizations, NGOs, and the civil society. Its mandate was to identify and formulate “building blocks for the governance of space resource activities as a basis for negotiations on an international agreement or non-legally binding instrument.” The Working Group adopted the final text of the building blocks on 12.11.2019. According to the proposed blocks, the objective of an international framework (“consistent with international law”) should be the creation of “an enabling environment for space resource activities that takes into account all interests and benefits all countries and humankind.” In this respect, the international framework should propose relevant recommendations and promote “the identification of best practices by States, international organizations and non-governmental entities.” It must be stressed that the potential impact of the space resources’ utilization issue for the maintenance of space security is recognized in the Building Blocks: According to the proposed Principles, the future international framework “should be designed to: . . . prevent disputes arising out of space resources” and “should provide that . . .space resources shall be used exclusively for peaceful purposes.”

Of course, the aforementioned concerns do not mean that commercial activities in outer space, of a private nature, should be discouraged. Such activities are clearly dictated by a new state of affairs in outer space and everything indicates that they are about to expand in the near future. Nevertheless, in the light of the desire of some states to put the famous “use of outer space” concept in a business perspective, it seems that current international space law might prove insufficient in this respect. This deficiency in the legal field can negatively affect international security with respect to outer space, including the Moon and other celestial bodies.

It must also be kept in mind that other important issues for an effective and secure commercial exploitation of outer space, in general, and the celestial bodies, in particular, – such as the protection of the space environment or the establishment of an effective space traffic management system – should also require, in the near future, the intervention of states through the undertaking of appropriate international action. What is more, new concepts emerge in space affairs: the long-term sustainability of outer space activities and the Space 2030 Agenda constitute additional factors and goals that push toward a rational and equitable use of outer space resources, which cannot be achieved through unilateral initiatives: an interesting model, in this respect, could be found in the International Telecommunication Union (ITU) Constitution, which dictates the “rational, equitable, efficient and economical use of the radio-frequency spectrum by all radiocommunication services” (Articles 12, 44).

---

## Conclusion

Space security is part of a broader security scheme in international affairs, the maintenance of which constitutes the fundamental purpose of the UN Charter. This requirement to maintain international security also applies in the context of space activities. In particular, the security of the celestial bodies presupposes the maintenance of a status quo defined by the current international legal framework. Under this framework, the celestial bodies must be used exclusively for peaceful purposes and constitute global commons, as they are not subject to “national appropriation by claim of sovereignty, by means of use or occupation, or by any other means.” What is more, the applicable norms with respect to activities on the celestial bodies are of international character, pursuant the obligation of states to “carry on activities in the exploration and use. . . [of] the Moon and other celestial bodies in accordance with international law, including the Charter of the United Nations.”

Although up to now it has been respected by states, said legal status of the celestial bodies does not seem to be fully adequate. The placement of weapons in empty space as well as on celestial bodies – despite their exclusively peaceful character – constitutes a threat which has preoccupied the international community for a long time. So far, the discussions and deliberations within the framework of the Conference on Disarmament have not been successful in adopting a binding international instrument, as negotiations for the adoption of a treaty on the prevention of the placement of weapons in outer space have failed thus far. This is due to fact that national security concerns are pushing some states to keep the debate on the placement of weapons in outer space open. At present, the adoption of voluntary transparency and confidence-building measures as well as the insistence by the General Assembly on the reference to the issue of the prevention of an arms race in outer space demonstrates that a consensus has already been formed within the international community on the need for multilateral action on this issue.

The growing desire of states and private actors to plan a commercial exploitation of the resources of the celestial bodies, once technology makes this feasible, can also be a source of frustration. Some states have already adopted national legal frameworks that regulate a unilateral exploitation of these resources, despite the international obligation of non-appropriation of the celestial bodies. On the other hand, the only existing collective exploitation regime is provided at present by the Moon Agreement, which has not been universally accepted by states. Consequently, a landscape is being formed in the context of which competition for space resources could trigger tensions and conflicts among states. It is worth mentioning that there are already deliberations in international *fora* (mainly at the COPUOS, but also in the context of The Hague Group) on a potential regulatory model of international character, despite disagreements as to its particular characteristics. Thus, the development of an international legal framework that will govern the commercial exploitation of space resources, ensuring, at the same time, a rational and equitable use of them in accordance with the spirit of Article I of the Outer Space Treaty, is a matter of security.

---

## References

- A/48/305 (1993) Prevention of an arms race in outer space. Study on the application of confidence-building measures in outer space. Report by the Secretary-General. 2 October. <https://digitallibrary.un.org/record/175346#record-files-collapse-header>. Accessed 28 Feb 2020
- A/68/189 (2013) Group of governmental experts on transparency and confidence-building measures in outer space activities. Note by the Secretary general, 29 July 2013. [https://www.unoosa.org/pdf/gadocs/A\\_68\\_189E.pdf](https://www.unoosa.org/pdf/gadocs/A_68_189E.pdf). Accessed 28 Feb 2020
- A/74/77 (2019) Group of governmental experts on further practical measures for the prevention of an arms race in outer space. Note by the Secretary-General, 9 April 2019. <https://undocs.org/A/74/77>. Accessed 28 Feb 2020
- Agreement Governing the Activities of States on the Moon and Other Celestial Bodies, New York, done 18 December 1979, entered into force 11 July 1984; 1363 UNTS 3; ATS 1986 No. 14; 18 ILM 1434 (1979)
- Celestial body. <https://www.yourdictionary.com/celestial-body>. Accessed 28 Feb 2020
- Charter of the United Nations (1945) 1 UNTS XVI. <https://www.un.org/en/charter-united-nations/>. Accessed 28 Feb 2020
- Draft International Code of Conduct for Outer Space Activities, Version 31 (2014) March. [https://eeas.europa.eu/sites/eeas/files/space\\_code\\_conduct\\_draft\\_vers\\_31-march-2014\\_en.pdf](https://eeas.europa.eu/sites/eeas/files/space_code_conduct_draft_vers_31-march-2014_en.pdf). Accessed 28 Feb 2020
- Draft Treaty on Prevention of the Placement of Weapons in Outer Space and of the Threat or Use of Force against Outer Space Objects (2008) CD/1839. <https://undocs.org/en/CD/1839>. Accessed 28 Feb 2020
- Draft Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects (2014) CD/1985. <https://undocs.org/en/CD/1985>. Accessed 28 Feb 2020
- Freeland S, Jakhu R (2009) Article II. In: Hobe S, Schmidt-T B, Schrogl K.-U (eds) Cologne Commentary on Space Law, vol 1. Outer Space Treaty, Carl Heymanns Verlag, Köln
- Hobe S (2009) Article I. In: Hobe S, Schmidt-T B, Schrogl K.-U (eds) Cologne Commentary on Space Law, vol 1. Outer Space Treaty, Carl Heymanns Verlag, Köln pp. 25–43

- Jackson-Preece J (2011) Security in international relations. University of London. <https://london.ac.uk/sites/default/files/uploads/ir3140-security-international-relations-study-guide.pdf>. Accessed 28 Feb 2020
- Jakhu RS, Pelton JN (eds) (2017) Global space governance: an international study. Chapter 12 global governance of space security. Springer, Cham
- Kyriakopoulos G (2015) The current legal regulation on the use of ASAT weapons under International Law and Space Law. In: Jakhu RS, Chen K-W, Nyampong Y (eds) Monograph series III: global space governance. McGill Centre for Research in Air and Space Law, Montreal, pp 599–618
- Luxembourg, Loi du 20 juillet 2017 sur l'exploration et l'utilisation des ressources de l'espace. Journal officiel, N° 674 du 28 juillet 2017. <http://data.legilux.public.lu/file/eli-etat-leg-loi-2017-07-20-a674-jo-fr-pdf.pdf>. Accessed 28 Feb 2020
- Lyll F, Larsen PB (2018) Space law. A treatise, 2nd edn. Routledge, London/New York
- Mosteshar S (2019). Space law and weapons in space. In: Oxford research encyclopedia, May 2019. <https://oxfordre.com/planetaryscience/view/10.1093/acrefore/9780190647926.001.0001/acrefore-9780190647926-e-74>. Accessed 28 Feb 2020
- Petrus M (2002) The use of force in response to cyber-attack on commercial space systems – reexamining ‘self-defense’ in outer space in light of the convergence of U.S. military and commercial space activities. *J Air Law Commer* 67:1213–1268
- Pop V (2001) Celestial body is celestial body is celestial body. . . In: A proceedings on the law of outer space, vol 44, pp 100–110
- Proposal by the United Arab Emirates on the work related to space resources utilization of the committee on the peaceful uses of outer space. A/AC.105/2019/CRP.17/19.6.2019. [https://www.unoosa.org/oosa/ooasadoc/data/documents/2019/aac.1052019crp/aac.1052019crp.17\\_0.html](https://www.unoosa.org/oosa/ooasadoc/data/documents/2019/aac.1052019crp/aac.1052019crp.17_0.html). Accessed 28 Feb 2020
- Proposal for the establishment of a working group for the development of an international regime for the utilization and exploitation of space resources. Working paper by Belgium and Greece. A/AC.105/C.2/L.311/4.3.2019. [https://www.unoosa.org/oosa/ooasadoc/data/documents/2019/aac.105c.2l/aac.105c.2l.311\\_0.html](https://www.unoosa.org/oosa/ooasadoc/data/documents/2019/aac.105c.2l/aac.105c.2l.311_0.html). Accessed 28 Feb 2020
- Ranganathan S (2016) Global commons. *Eur J Int Law* 27:693–717
- Sackstender KR, Sanders GB (2007). In-situ resource utilization for lunar and mars exploration. In: 45th AIAA aerospace sciences meeting and exhibit, Reno, 08 January 2007–11 January 2007. <https://arc.aiaa.org/doi/pdf/10.2514/6.2007-345>. Accessed 28 Feb 2020
- Schrogl K-U, Neumann J (2009) Article IV. In: Hobe S, Schmidt-T B, Schrogl K.-U. (eds) Cologne Commentary on Space Law, Vol 1, Outer Space Treaty, Carl Heymanns Verlag, Köln
- Space Security Index (2019) Space security index 2019, 16th edn. Waterloo Printing, Waterloo
- Takaya-Umehara Y (2010) TCBMs over the military use of outer space. *Acta Astronaut* 67(9–10): 1299–1305
- The Hague International Space Resources Governance Working Group (2019) Building blocks for the development of an international framework on space resource activities, 12 November. <https://www.universiteitleiden.nl/binaries/content/assets/rechtsgeleerdheid/instituut-voor-publiekrecht/lucht%2D%2Den-ruimterecht/space-resources/bb-thissrwg%2D%2Dcover.pdf>. Accessed 28 Feb 2020
- Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies, adopted on 19 December 1966, opened for signature on 27 January 1967, entered into force on 10 October 1967, 610/U.N.T.S./205
- Tronchetti F (2015) Legal aspects of the military uses of outer space. In: Von der Dunk F, Tronchetti F (eds) Handbook of Space Law. Edward Elgar, Cheltenham/Northampton, pp 331–381
- UN System task team on the post-2015 UN Development Agenda (2013) Thematic think piece: global governance and governance of the global commons in the global partnership for development beyond 2015. [https://www.un.org/en/development/desa/policy/untaskteam\\_undf/thinkpieces/24\\_thinkpiece\\_global\\_governance.pdf](https://www.un.org/en/development/desa/policy/untaskteam_undf/thinkpieces/24_thinkpiece_global_governance.pdf). Accessed 28 Feb 2020
- UNGA A/RES/68/50. Transparency and confidence-building measures in outer space activities. 5 December 2013. [https://www.unoosa.org/pdf/gares/A\\_RES\\_68\\_050E.pdf](https://www.unoosa.org/pdf/gares/A_RES_68_050E.pdf). Accessed 28 Feb 2020



---

## Part II

# Space Security Policies and Strategies of States



# Space Security Policies and Strategies of States: An Introduction

# 19

Jana Robinson

## Contents

Introduction .....	359
Space Security Policies and Strategies of States .....	360
Conclusion .....	364
References .....	365

## Abstract

This chapter provides an introduction to Part 2 of the second edition of the Handbook of Space Security entitled “Space Security Policies and Strategies of States.” It covers expert views on space security policies of established spacefaring nations, including the United States, China, Russia, European countries, Japan, and India. It also reviews space security policies of emerging space powers – Brazil, Israel, the UAE, Poland, and Azerbaijan – to showcase a wide range of space policy approaches to this strategic security portfolio. The chapter likewise includes overviews of European and Asia-Pacific approaches to space security issues. These approaches range from strict emphasis on the peaceful uses of outer space (e.g., Brazil and the UAE), to space as a key element of national security and defense (e.g., U.S., Russia, China, and Israel), or a combination of both (e.g., India).

## Introduction

In contrast to the Cold War period, the space environment today involves some 88 countries and government consortia with different strategic objectives and levels of economic and technological development (Euroconsult 2019). There are also an ever-growing number of commercial satellite operators. Earth observation,

J. Robinson (✉)

Space Security Program, Prague Security Studies Institute (PSSI), Prague, Czech Republic  
e-mail: [jrobinson@pssi.cz](mailto:jrobinson@pssi.cz)

communications, and satellite navigation, originally supporting mainly military activities, are now part of day-to-day civilian and commercial life. As a result, there is a growing concern regarding how to best preserve safe, stable, and sustainable space operations over the long term.

Established spacefaring nations like the United States, Russia, and some European countries have developed national policies and strategies that address space security issues. This portfolio is also rich with the agenda of other space powers, such as China. Several nations, including Japan, are integrating space security into their broader national security and foreign policy agendas. At a multilateral level, a body of principles and rules governing space activities, including a unique international status of outer space and celestial bodies, was established during the second half of the twentieth century. Implementation of these principles and rules has, however, lagged for a number of reasons, including the “asymmetric” interests in space, the growing connectivity between terrestrial tensions and space security, the lack of a track record on the multilateral management of an incident in space, and other considerations.

This section of the Handbook introduces different approaches to managing space security on the part of select spacefaring nations (i.e., the United States, Russia, China, Japan, India, Israel, Brazil, the UAE, Poland, and Azerbaijan). It also includes overviews of European and Asia-Pacific approaches to space security issues. As it will be evident from the content of various chapters, there is, as yet, no consensus on what issues constitute the space security portfolio. There are also significant differences in the main focus of individual national space programs. There is, however, an evident requirement for an improved dialogue on major space security issues and enhanced international collaboration on the more contested aspects of space operations.

---

## **Space Security Policies and Strategies of States**

The emphasis on the peaceful uses of outer space coexists with the underlying role of space as an instrument of national security and international prestige. Threats to space assets and activities, both natural and man-made, are multiplying, as evidenced by events such as China’s repeated antisatellite (ASAT) tests, Russia and, most recently, India (in March 2019), or close approaches by Chinese and Russian satellites to foreign spacecraft.

Man-made threats include intentional disruption of satellite services and even attacks on space assets. Intentional jamming could have damaging military, political, and commercial knock-on effects. A prominent example of such deliberate interference has been the repeated jamming of Eutelsat satellites by a source located on Iranian territory. Other threats include directed or kinetic energy ASAT attack or cyber assaults. Cyber-attacks against satellites and ground stations are a rapidly growing concern – and vulnerability – and should be added to the list of political and budgetary challenges to enhance security in both the space and the cyber domains. Although there have not, as yet, been any serious consequences (at least confirmed

reports) resulting from such incidents, these events have highlighted the need for establishing not only national procedures but also diplomatic processes to facilitate the smooth and efficient management of these types of actions internationally. Although space threats emanating from natural hazards or technical issues warrant genuine concern, the intentional disruption of, or damage to, space assets and systems would generally involve larger – sometimes far larger – geopolitical stakes.

In the *United States*, space policy has remained relatively consistent over the past 60 years with a focus on international cooperation, peaceful intention, and development of outer space for the common good of all humankind. ► [Chap. 20, “War, Policy, and Spacepower: US Space Security Priorities”](#) by Everett C. Dolman explains how throughout this time, every policy has reserved the right of self-defense in space while interpreting military activity rather broadly. Yet, the 2017 National Security Strategy made a notable shift, in particular with regard to the security aspects and reviving, the National Space Council. The US Space Policy Directives 1 and 2 aim at fostering reinvigorating America’s human space exploration, and commercial activities through appropriate regulatory framework, while Space Policy Directives 3 and 4 address the creation of space traffic management and the establishment of a Space Force, respectively. The Space Force has become the sixth branch of the US military, housed within the Department of the Air Force. In addition, the US Space Command was reestablished to organize military space operations. The US leadership now believes that it is irresponsible to rely on the better intentions of its adversaries, international agreements, and deterrence to guarantee its national space interests. The new policy makes clear that space is now considered a warfighting domain, and the USA will prepare itself to fight and win military conflicts that might occur in this domain.

Outer space has also become an important area through which *Russia* aims to rebuild its global status and prestige as a space power, including its efforts to shape global norms. Russia considers outer space predominantly as a strategic region to enhance its military capabilities on Earth, provide intelligence and communication functions, and achieve international esteem. Nicole Jackson describes how Russia reacts to US strategy and continues to develop counterspace technologies (e.g., electronic weapons that can jam satellites) to provide the country with an asymmetrical edge to offset US military advantages. Accordingly, military efforts are but one part of a complex set of tools, employed to navigate what Russia perceives as an increasingly hostile world. Back in 2011, Russia brought about certain institutional modernizations creating the Russian Aerospace Defence Forces to conduct its space security-related activities. Recently, in March 2018, the Russian Defense Minister Sergey Shoigu stated that Russia must deploy a modern fleet of military satellites to support its army and navy. He stated: “only with support from space will it be possible for the Armed Forces to reach maximum effectiveness.” However, its economic, military, and technological weaknesses, compared to those of the US and NATO, have led Russia to pursue asymmetrical tactics and focusing on bilateral relations as well as pushing its agenda through the United Nations.

Formerly part of the USSR, *Azerbaijan* has been involved in space activities for some decades. The country has an agency, the Azerbaijan National Aerospace

Agency (ANASA) created in 1992. Its recent activities are part of the space strategy “Azerbaijan 2020” which aims to develop the Azerbaijani space industry and own satellites.

Space security and defense discussions in *Europe* have been supported by an existing space security culture of the Western European Union, as explained by Alexandros Kolovos. Over the past several years, the European Union (EU) has formulated a space security strategy, including in the 2018 proposal for a Regulation for a Space Program for the EU which is based on the 2016 Space Strategy for Europe. One of the main goals of the Space Strategy is to “Reinforce Europe’s autonomy in accessing and using space in a secure and safe environment.” In order to realize the security objective, the EU Regulation proposes the development of Governmental Satellite Communications (GOVSATCOM) and Space Situational Awareness (SSA) programs to accompany Galileo and Copernicus. At the same time, the European Space Agency (ESA) has more explicitly formulated its space security policy, as reflected in the “Elements of ESA’s Policy on Space and Security” and the safety and security program adopted at the ESA Ministerial Council in 2019. In addition to ESA and the EU policy and programmatic developments, NATO Defence Ministers approved in 2019 its first ever space policy. The NATO Secretary General Mr. Stoltenberg stated that the premise for the space policy is that: “Space is part of our daily life here on Earth – it can be used for peaceful purposes, but it can also be used aggressively.” The authors of these chapters describe the institutional space and security policy developments in Europe that have taken place in parallel with the policies of the individual European countries. These include the 2019 French Space and Defence Strategy and other trends in the main European space powers, as well as in emerging ones, such as Poland. Overall, European space and security governance is multifaceted, thereby posing a major challenge to effective mutual cooperation among the EU, ESA, and the European States.

Asia is the world’s second-largest defense spender while it is becoming increasingly active in space. Japan, China, and India have been the most prominent space actors in this region. Dr. Rajagopalan explains how the geopolitical and military competition in Asia has an impact on the space efforts of these countries. The growing space competition manifests itself by the rapidly growing development of counterspace capabilities, such as kinetic ASAT missiles, electronic and cyber warfare capabilities, as well as new efforts at creating specialized military agencies devoted to space utilization. There are three key drivers to space conflict in Asia, according to her – increasing use of space for military purposes; civilian use that could also lead to conflict because of congestion and competition; and investments in military technologies such as those for ASAT weapons and missile defense.

Concerning *China*, its space ambitions are long-term and strategic, externally emphasizing stability and publishing its 5- and 10-year plans for space. China has been steadily and systematically rising as a major space power and the world has witnessed, among other achievements, the landing of an unmanned mission on the near side of the Moon using its Chang’e 3 in December 2013, and the Chang’e 4 landing on the far side of the lunar surface in January 2019. Over the past several decades, the relationship of space and national security has been evolving as part of a

broader ongoing assessment of the role of information in future warfare, as explained by Dean Cheng. Due to the People's Liberation Army's (PLA) attention to information and communications technologies, the centrality of space dominance has grown as well. In 2015, China established the PLA Strategic Support Force (PLASSF) which saw the integration of the PLA space, cyber, and electronic warfare capabilities, and considered a significant domestic achievement concerning China's preparedness for multidomain future warfare. For the PLA and China's security decision-makers more broadly, the Information Age and the Space Age are inextricably linked. Both have been heavily influenced by the growth in computing power and the role of telecommunications. This has gained impetus as Information and Communication technologies (ICT) have become a key element in overall national power and, especially, military capabilities.

Kazuto Suzuki explains how *Japan's* space policy has been influenced significantly by the overall foreign and security policy. Since the inception of its space activities, Japan has been reluctant to engage in security-related uses of space, largely due to its Constitution. This attitude has evolved over the past few years. In 2013, the country updated the Basic Space Plan which was released in 2009. The revised Plan emphasized the need for new opportunities for the involvement of Japan in international efforts to address the most pressing space security-related challenges of the twenty-first century. At the end, the 2013 update, and its subsequent revision in 2015, marked the reorientation of Japan's space program towards tackling the changes in the regional security environment. The latest version of the Basic Space Plan of 2017 aims at responding to the growing threat of ASAT weapons and the increasing quantity of space debris by putting emphasis on space security. Space security, through the strengthening of security capabilities and the Japan-US alliance, ensures the stable utilization of outer space.

*India* has acquired multifaceted space capabilities with dual-use applications (i.e., both civilian and military). These include satellite communications, Earth observation, and navigation. Over the years, Indian Space Research Organisation (ISRO)'s program has matured significantly and, at present, India's space program is regarded as one of the important space programs in the world. From launching small satellites to undertaking a successful mission to the Moon and Mars, India has excelled in almost all areas of space experimentations. India is also proposing to undertake its first human space mission by 2022. Ajey Lele describes how India has made significant investments towards establishing its military architecture owing to its strategic needs. Space technologies are finding increasing relevance in strengthening this architecture, essentially as a force multiplier. The March 2019 ASAT test clearly communicated India's intention and capability to use space for military purposes. Soon after the test, India has announced plans to establish a Defence Space Agency marking a shift in the evolution of the Indian space strategy.

*Israel*, like many other countries, wants to exploit the dual-use aspects of space technologies to advance economic, commercial, security, civil, and foreign policies. Deganit Paikowsky and co-authors describe how, in the past 30 years, Israel developed an indigenous space capability to develop, launch, operate, and maintain satellites in two main areas: Earth observation and communications, including the

ground segment of communications satellites. As security in the region has been the country's key concern, Israel's military space program has, throughout its history, been the main driver of the country's space activities. It has, however, also resulted in the growth of the commercial space sector. Israel has expanded, in recent years, its cooperation with international partners as well as established a civilian space policy backed by modest government funding. What began as a purpose-focused defense necessity has blossomed into a diversified amalgam of enterprises, academia, and government dealing with a broad spectrum of space endeavors. Within the context of protecting and encouraging this nationally important ecosystem, Israel considers international space security, safety, and sustainability to be of key importance.

The *United Arab Emirates* (UAE) has realized the increasing importance of the space sector, and supported its continuous growth at a regional and global level. Due to the increasing number of activities in the space industry, and the growing rate of national investments, combined with the technical, economic, and political developments in the sector, the UAE government has pointed towards establishing a national policy and regulatory framework for space activities, aligned with national and international policies and best practices. Naser Al Rashedi and co-authors explain how the UAE actively contributes in utilizing space to achieve long-term sustainability. In line with this mandate, the UAE National Space Strategy 2030 has been reviewed to ensure its alignment with the 17 sustainable development goals (SDGs-2030), the UNCOPUOS Long Term Sustainability Guidelines, and the four pillars defined in the revised zero draft of a "Space2030."

Concerning South America, and despite the challenges to the economy in the region, *Brazil* has managed to sustain growth since the end of 2017 with an industrial production growing slowly. Olavo Bittencourt Neto and Daniel Freire e Almeida describe the evolution of the Brazilian space law, policy, and initiatives related to space security. As an emerging space faring nation, Brazil acknowledges the crucial importance of space activities to the exercise of its national sovereignty. For a territory of 8,514,215.3 km, home of over 200 million people, appropriate satellite coverage is always a challenge. Through the years, successive federal governments have invested time, capital, and people on strategic initiatives focused on local needs, ranging from remote sensing to telecommunications capabilities. Nevertheless, space activities remain an expensive endeavor, and access to crucial technology is often limited by political and legal constraints. Thus, Brazil has recognized that international cooperation is frequently required to secure specific services and expertise, leading to the negotiation of agreements with foreign partners.

---

## Conclusion

The growing ambitions of countries in space have increasingly been accompanied by concerns over the need to protect space systems that enable vital global information flows. All space actors, no matter their level of capability, strive to have a stake in the

---

global evolution of space activities. That said, it remains a reality that there is growing divergence in propositions of how to treat risks and threats to the operational space environment by major space powers and their allies.

The shared interests of spacefaring nations, as well as those of the multitude of beneficiaries of space activities worldwide, can only be accomplished by pursuing a sustainable model of global space governance that is based on transparency and the rule of law. Although different countries emphasize varying space capabilities, strengthening space security should be a priority for all of them.

---

## References

Euroconsult (2019) Government Space Programs. Benchmarks, Profiles & Forecasts to 2028





# War, Policy, and Spacepower: US Space Security Priorities

# 20

Everett C. Dolman

## Contents

Principle and Practice in US Space Policy .....	368
Current US Space Policy .....	380
Conclusion .....	383
References .....	384

## Abstract

Official US space policy has remained relatively consistent over the last 60 years. Beginning with Eisenhower, every administration has stressed international cooperation, peaceful intention, and development of outer space for the common good of all humankind. Significantly, every policy has also reserved the right of self-defense in space. In practice, the United States has interpreted these policy constants, particularly regarding military activity, quite broadly. The 2017 National Security Strategy (NSS) made a notable and historically unique public change in emphasis, however. In his preface, President Donald Trump declared that “we are charting a new and very different course” consistent with a larger international policy of “America First.” This chapter describes continuity and change in space policy over the last 60 years, summarizes the current administrations space directives, and discusses current proposals for a separate military space force within the U.S. Department of Defense.

Official US space policy has remained relatively consistent over the last 60 years. Beginning with Eisenhower, every administration has stressed international

---

E. C. Dolman (✉)  
Air Command and Staff College, Air University, Montgomery, AL, USA  
e-mail: [everettdolman@gmail.com](mailto:everettdolman@gmail.com)

© This is a U.S. government work and not under copyright protection in the U.S.; foreign copyright protection may apply 2020 367  
K.-U. Schrogl (ed.), *Handbook of Space Security*,  
[https://doi.org/10.1007/978-3-030-23210-8\\_124](https://doi.org/10.1007/978-3-030-23210-8_124)

cooperation, peaceful intention, and development of outer space for the common good of all humankind. Significantly, every policy has also reserved the right of self-defense in space. In practice, the USA has interpreted these policy constants, particularly regarding military activity, quite broadly. The 2017 National Security Strategy (NSS) made a notable and historically unique public change in emphasis, however. In his preface, President Donald Trump declared that “we are charting a new and very different course” (National Security Strategy of the United States of America, December 2017, p. i). He asserted the USA would continue to pursue cooperation, but “in an extraordinarily dangerous world” only via a “balance of power that favors the United States, its allies, and our partners” (Ibid, pp. i; ii). To ensure no misinterpretation, just prior to his distinctive signature, he declared: “This National Security Strategy puts America First” (Ibid, p. ii).

The rapidly evolving US space policy is currently in flux. President Trump has issued four Space Policy Directives (SPDs), the last ordering establishment of a separate and equal sixth branch of military service within the Department of Defense (DOD). The new Space Force will be responsible for warfighting operations *in* and *from* space. His administration has not yet released the full text of a National Space Security Strategy (NSSS), but in March of 2018 the White House announced a new National Space Policy (NSP) and released several fact sheets summarizing its contents. In the meantime, the US Congress has yet to debate the details of – or approve – a space force structure or budget. With so little of the coming policy settled, the first task in assessing future probabilities is to understand the past. Accordingly, this chapter begins with a brief survey of previous US military space policies. A review of the space portions of the Trump administration’s National Security Strategy (NSS), White House descriptions of the pending Trump NSP, and Trump’s SPD-1 through 4 follows. An assessment of the current Space Force proposal completes the chapter.

---

## Principle and Practice in US Space Policy

In his 1960 Farewell Address, President Eisenhower warned of an insidious growth in the partnership between business, technology, and the military – what he termed the military-industrial complex. Just 15 years earlier, as World War II was drawing to a close, the consensus was quite the opposite; a closer relationship was needed. On 12 November 1945, Chief of the Army Air Forces H. H. “Hap” Arnold provided a summary of that view in a report to the Secretary of War: “The conclusion is inescapable that we have not yet established a balance necessary to ensure the continuation of teamwork among the military, other government agencies, industry, and the universities” necessary to successfully prosecute future wars (Ware 2008). This led to the establishment of a scientific think tank, initially based in the Douglas Aircraft company, called Project RAND (a contraction of the term research and development). Tucked into that 1945 report, General Arnold warned the Secretary that ballistic missiles for deterrence and satellites for surveillance and

early warning would be the best means for preventing a future Pearl Harbor-like surprise attack (Spires 1998). RAND's first Air Force-sponsored report, released in March 1946, was titled *Preliminary Design for a World-Circling Spaceship* (RAND 1946). War was going to extend to the heavens, and America would not be left behind. Thus began an alternating policy history of pursuing and eschewing military war-making in, to, and from space.

In the 1940s and 1950s, America was obsessed with new technology and enamored with the possibilities for society and war. In the US military, this meant adapting the four great inventions of WW II, Germany's medium range ballistic missile, British radar technology, American electronic computers, and nuclear weapons for what would surely become a radical new way of war (Walter McDougall, in his Pulitzer Prize-winning book, asserts that all the world's space programs were born of these wartime inventions. . . .*the Heavens and the Earth: A Political History of the Space Age* (New York: Basic Books, 1985), p. 6). In fact, it was the confluence of these technologies that allowed humanity to achieve the means to go into space. A rocket that could lift an operational payload to orbital altitude, a radar-based guidance system that could place the payload into precise orbit, and a method for making necessary planning and real-time operational calculations were needed. But it was the perceived need for a reliable and certain means to carry the tremendously destructive (and expensive) nuclear bomb to its destination that made the cost of researching, developing, and fielding InterContinental Ballistic Missiles (ICBMs) necessary. The rocket was the motive force that could travel at speeds no defensive system could intercept, while the radar and computer allowed precision targeting over vast distances.

Within the US military, initial development exposed a predominantly Army-centric view of rocket power. Much of the German V-2 development team, to include Director Werner Von Braun, along with equipment and scientific records, were captured in Operation Paper Clip and set to work in the USA to build its own ballistic missile program (Neufeld 2007). The Army perceived the V-2 as long-range artillery, hence within its mandate. Space launch vehicles would be a useful spin-off. The Navy and Air Force emphasized the potential for satellites to support terrestrial operations through intelligence, surveillance, and reconnaissance (ISR), navigation, weather, and communications support, and needed rockets to launch them. Progress for both slowed under the New Look fiscal austerity policies of the Eisenhower administration, as military budgets were tightly squeezed and lower priorities were shelved.

The USA had spent a great deal of money developing nuclear weapons and the means to deliver them through the air. Eisenhower felt a return on that investment should be leveraged. The Massive Retaliation doctrine of the 1950s stated that any transgression against the United States, no matter how slight, *could* be met with a nuclear response. With such a terrifying threat, the administration reasoned that conventional military capabilities could be pared to the bone, as no rational actor would risk such punishment. (Of course, they did, and small-scale threats and conflicts were tolerated so long as they didn't escalate to the need for nuclear strikes. Once the USSR became capable of countering the US with nuclear warheads

of its own, larger conventional conflicts became safe from nuclear reprisal so as to not start a global nuclear exchange.) Accordingly, the Air Force retained the largest share of military spending in this period because of its strategic nuclear strike mission, to be carried out entirely by the long-range bombers of Strategic Air Command (SAC). ICBMs were not then as accurate as a bomber, and so it eschewed ballistic missile development. But aircraft were vulnerable to countermeasures, primarily from rapidly advancing Russian Surface-to-Air Missiles (SAMs), whereas a ballistic missile reentering the atmosphere from space was not. Should the Army or Navy achieve a ballistic missile capable of striking deep into Soviet territory with accuracy, the Air Force's strategic strike monopoly, and the percentage of the defense budget allocated to it, would erode. Through a series of bureaucratic and political maneuvers, by the mid-1950s the Air Force usurped much of the Army's ballistic missile mandate and, under the guidance of General Bernard Schriever, began an ICBM program in earnest. (An excellent source is Neal Sheehan 2010.)

Despite more than a decade of interest, the first military satellite development program (WS-117L reconnaissance satellite) was not authorized until 1954, and then only for basic research and preliminary tests (Stares, *Militarization*, pp. 30–3). The following year, a civilian satellite project was announced to coincide with the 1957 International Geophysical Year (IGY) competition calling for a satellite launch by the end of the year (Ibid., pp. 33–5). The Soviet Union proclaimed it would enter as well, proof of its accelerating scientific advancement, but most Americans believed the announcement was pure bravado – their technology was too far behind the USA to be taken seriously. That confidence was shattered on 1 October 1957.

The launch of *Sputnik-1* caused a national hysteria. The capability to put a satellite into a precise orbit was evidence of the capability to reach out and target any city on the globe. The simple beep-beep transmission that could be heard from *Sputnik* every 90 min as it passed overhead affirmed that no place in America was safe from nuclear war.

Nonetheless, significant evidence has been accumulated to allow some authors to suggest the USA secretly prompted the Soviets into going first (see e.g., Mieczkowski 2013; Johnson-Freese 2007). Under international law, state sovereignty extends into the airspace above its territory. Whether that sovereignty extended into outer space was hotly contested. Recognizing that its illegal U-2 flights over the USSR would end as soon as the Soviets could defend against them, and desperately in need of a replacement for the ability to monitor the closed-off state's nuclear capabilities, spy satellites were the obvious next step (as happened to Gary Powers in 1960, ending airborne reconnaissance of the Soviet Union). Since *Sputnik's* orbit passed over the much of the globe, America immediately declared the action established a precedent – the right of free overflight by orbiting spacecraft worldwide. The Soviets assented. State sovereignty would extend to somewhere between the highest altitude of powered flight and the lowest altitude of sustainable orbit (a line still not established in international law, creating an ambiguous zone between the two criteria). Much like international waters, space would be a global commons where innocent passage was open to all. The event proved so advantageous for US security needs that the Eisenhower administration

has been credited with purposely holding back space development to ensure that his “Open Skies” vision would be realized (Johnson-Freese 2009). This position makes the US administration seem too clever by half. The government appeared genuinely unprepared for the public reaction, and the space program – such as it was – lagged significantly behind.

Of note, Von Braun had practically begged to be allowed to use an Army Redstone rocket to place a satellite into orbit as soon as possible (McDougall, *Heavens and Earth*, p. 119). In a 1954 report titled “A Minimum Satellite Vehicle,” he requested just \$100,000 to accomplish the feat using existing equipment and technology. Because the Redstone was an upgraded version of the V-2 and Von Braun had a shady past in the Nazi Party and SS, to allow him to do so would have put a too militaristic face on American space ambitions. His requests were denied. With *Sputnik’s* October surprise, however, and the follow-up launch of a much larger *Sputnik* carrying a live dog (Laika, who as planned burned up on reentry), accelerated the crisis. After the original IGY entrant, Project Vanguard, suffered a series of high profile setbacks and an embarrassing launch failure in December, the Army was finally authorized to launch an alternative satellite on a modified Redstone rocket (dubbed Jupiter-C). Explorer-1, weighing just 3.5 pounds – a fraction of the 135-pound first *Sputnik* – achieved orbit on 31 January 1958.

The close association with ballistic missiles and national space programs was clear. No state has yet developed a space launch vehicle that cannot trace its technological lineage to ballistic missile program. To counter international concern, and recognizing that it was much further behind in space exploration – particularly heavy-lift – than its Cold War rival, America publicly and completely bifurcated its space program into purely civilian and military sectors (Stares 1985). While the civilian side may have perceived scientific competition in space as a route to peaceful cooperation and mutual benefit, the US military had an entirely different view. Access to space was a harbinger of future wars.

Speaking to the National Press Club shortly after *Sputnik*, Chief of Staff General Thomas White declared “whoever has the capability to control space will likewise possess the capability to exert control over the surface of the earth . . . We airmen who have fought to assure that the United States has the capability to control the air are determined that the United States must win the capability to control space” (Futrell 1985). Shortly thereafter – perceived by the other services as a bid to ensure that space would be its exclusive purview – Air Force leadership inserted the word *aerospace* throughout its doctrine to cement the notion that air and space were a continuous and indivisible operational medium (Ibid., 64, 68). From a warfighting perspective, this meant developing and deploying *piloted* spacecraft that could mimic established aircraft operations. A push was on to fast-track space fighters, bombers, and transports, a view that would have unsustainable ramifications in the next decade.

The Air Force’s vision was not shared by the other services. Army General James Gavin insisted the nation must develop an unmanned satellite interceptor system “. . . otherwise it will be helpless before any aggressor equipped with armed reconnaissance satellites” (quoted in Stares, *Militarization*, p. 49). Army Air

Defense Artillery (ADA) forces saw space defense as a natural extension of its own inherent capabilities. In 1959, Admiral Arleigh Burke, Chief of Naval Operations, proposed to the Joint Chiefs a combined military space agency, a precursor of future unified space commands, based on the shared “indivisibility of space” (Spires, *Beyond Horizons*, p. 76). The Navy and Army had legitimate needs for space support and capability, and proposed sharing equally in the new mission as a cost-saving measure, but parochial service rivalries were not yet ready for sharing domain responsibilities.

The 1958 National Security Council (NSC) Directive 5824, “U.S. Policy on Outer Space,” concerned the development of military reconnaissance satellites and highlighted the need to ensure any political response would be as favorable to the USA as possible. Although the decision had already been made to separate the civilian side of government space duties, to allay potential domestic and international objections, follow-on NSC Directive 5814/1, “emphasizing denying Soviet space superiority,” was uncomfortably provocative (Ibid., p. 64).

Early focus was on the development of reconnaissance satellites, with the caveat that any program must be politically reassuring. This left much room for interpretation. In accordance with the logic of the ancient Roman adage *si vis pacem para bellum*, military space activities must be conducted with peaceful *intent*: to deter war. Thus several prospective programs aimed at preparation to fight a future war in space were clustered under the broader program titled Dyna-Soar (a compression of Dynamic Soaring that, in the context of aggressive cutting-edge science, was an unfortunate name). (Eventually eXperimental plane 20 (X-20), a rocket-launched piloted space bomber that could glide back to earth held exclusive title to the name Dyna-Soar. For a full history, see Houchin 2006) Among these was an Air Force satellite interceptor program called SAINT (another compression). Although President Eisenhower would not authorize any actions beyond concept development, his successor would have fewer qualms.

Running against Eisenhower’s fiscal policies leading to what he perceived as insufficient funding of non-nuclear military capabilities, Senator John F. Kennedy campaigned on reinvigorating all of America’s warfighting capabilities. Speaking on the campaign trail, Kennedy made it clear that war in space was included: “We are in a strategic space race with the Russians and we are losing . . . Control of space will be decided in the next decade. If the Soviets control space they can control the earth . . . we cannot run second in this vital race” (from an interview in *Missiles and Rockets* magazine, cited at <https://history.nasa.gov/SP-4225/documentation/competition/competition.htm>). Citing the Soviet’s clear lead in space launch capability, Kennedy was especially persuasive on the charge that Eisenhower’s administration stood by while the Soviets gained a distinct advantage in ballistic missiles. Famously stoking fears over a growing “missile gap,” Kennedy eked out a victory over Eisenhower’s political heir, Vice President Richard Nixon (well documented in Christopher Preble 2004).

Despite later admission, there had been no missile gap – or if there had, it was distinctly in favor of the USA – uncertainty over Soviet intentions enhanced military arguments. The Soviet Union was testing warfighting systems *to* space – including

the exotic MiG 105 spaceplane – and armed satellites *in* space. A particular concern was indications of a Fractional Orbital Bombardment System (FOBS), an orbiting platform that could release nuclear warheads with trajectories that would bypass American defenses arrayed along the northern Arctic front (Mowthorpe 2004; Stares, *Militarization*, pp. 99–100). Satellites were starting to provide invaluable intelligence, and early-warning was increasingly reliant upon them. In 1962, the Soviets began an intensive political campaign in the UN to prohibit space reconnaissance over sovereign territory (Stares, *Militarization*, pp. 62–71). With the Dyna-Soar Program now focused exclusively on a piloted military spaceplane that could conduct combat operations in space and return safely to the earth and a Manned Orbiting Laboratory (MOL) program the Russians insisted was a military reconnaissance platform, the Kennedy administration pressured the Soviets into dropping their insistence on a satellite reconnaissance ban and to agree with the USA that nuclear weapons should not be based in outer space.

Vice President Lyndon Johnson inherited the Kennedy/McNamara military space program after the tragic assassination of President Kennedy. His administration's official policy continued the general principles of freedom of space and active pursuit of arms control arrangements and international cooperation while developing appropriate and necessary military means to defend American interests in space (Stares, *Militarization*, p. 93). This standard has generally been held throughout all successive administrations, the differences hinging on perceptions of appropriate and necessary military actions.

Johnson also inherited a civilian race to the Moon, a massive conventional arms build-up coupled with a rapidly escalating commitment to a war in Vietnam, and a nuclear arms/ICBM race that had spiraled out of control after the Russian humiliation in the Khrushchev/Kennedy Cuban missile crisis – all putting a colossal strain on the federal budget that jeopardized his signature Great Society socioeconomic transformation. For their part, the Soviets were saddled with similar problems. Despite a foundering economy, they had the same space and arms race commitments as the USA as well as a Vietnam parallel with the continued expense of suppressing anti-Russian sentiments in Eastern Europe. Something had to go, and so by 1964 both sides willingly engaged in serious negotiations to curtail a potentially ruinous race for space weapons.

The 1967 Outer Space Treaty (OST) established outer space as a global commons, free from national appropriation, and formalized the language that would continue to dominate international agreements regarding space policy. Space was the common heritage of all mankind, and the benefits of space exploration should be shared by all. The OST also prohibited the stationing in earth orbit or on celestial bodies of weapons of mass destruction, defined as “nuclear, biological, chemical, and radiological,” but did not ban the transit of these warheads through space on the way to their intended targets ([www.unoosa.org/pdf/publications/STSPACE11E.pdf](http://www.unoosa.org/pdf/publications/STSPACE11E.pdf)).

The USA had by this time cancelled Dyna-Soar and the MOL, and transferred its astronauts to support NASA. For its part, the Soviets declared they had no interest in a Moon race with the Americans, nor any intent to wage war in space.

For public consumption, the two Cold War superpowers had entered into a period of non-military cooperation in space. They even agreed to a few joint exploration events that it was hoped could spill over to cooperation in other, terrestrial areas.

In practice, however, not so much. The nuclear arms race accelerated. From a few hundred medium and intercontinental missiles in 1960, by the end of the decade each side possessed more than 10,000 nuclear warheads, a number that would double again before the end of the 1970s. The USA would continue its war in Vietnam, expanding it throughout Southeast Asia before finally coming home in 1973. The Russians would brutally put down the Czech uprising in 1968. Publically, at least, the race to militarize space was curtailed.

The Richard Nixon/Gerald Ford and James Carter administrations continued the public policies articulated formally under the OST and entered into the first significant Strategic Arms Limitation (SALT I and II) talks with the Soviets. The Nixon administration also concluded a treaty banning anti-ballistic missiles (ABMs) in 1972. With serious economic problems emanating from the previous decade, the Moon programs were cancelled. While policy focused again on fiscal constraint and defusing terrestrial conflicts, in military space, this was a significant era of ASAT experimentation.

The USA had already tested high altitude nuclear detonations in space under the STARFISH PRIME program over the South Pacific, but found the effects to be too indiscriminate and persistent to be of practical warfighting value (Plait 2019). The Air Force co-orbital SAINT interceptor program had been discontinued, but the Navy continued testing its submarine-based Polaris missiles as possible direct ascent ASATs into the 1970s (Stares, *Militarization*, pp. 106–129). The Soviet Union, recognizing the enormous enhancement of US military capability provided by its military satellites, conducted intensive testing of a large co-orbital ASAT from 1968 into the 1980s.

The Soviet ASAT, a massive (2,500-plus kg) conventional explosive launched aboard an SL-11 rocket into the same orbit as its target. Once in sufficient proximity, it detonated, creating a debris field that obliterated the satellite. The Soviets conducted at least 20 on-orbit tests through 1982, successfully destroying the target satellite in more than half of its attempts (Baker 2005). Although it declared a moratorium on further tests in 1983, the Soviet Union then Russia continued to use the ASAT booster to place various military satellites into orbit and maintained the warhead in storage for decades. In 1975, the third Salyut-series space station was equipped with a 23 mm cannon, adapted from a Tupelov bomber tail gun (Zak 2015). The station successfully test-fired the gun remotely that year, and may have equipped follow-on stations with modified air-to-air missiles.

President Nixon could afford little attention to the military ramifications of Russia's offensive space capability. He had run successfully a second time, in both cases on the promise that that he would extract the USA from Vietnam, which he finally did in 1973. But in that second campaign he authorized a break-in of the opposition party's headquarters in the Watergate Hotel. The resulting scandal ultimately forced him to resign. He was succeeded by Vice President Gerald Ford, who ran out Nixon's term. His main priority was the domestic economy, specifically



suppression of rampant inflation. Faced with the clear Soviet ASAT asymmetry, in the last month of his term he directed the Defense Department to develop an operational anti-satellite capability (Stares, *Militarization*, p. 175).

President James Carter's administration was keenly interested in negotiations to slow the continuing rise in nuclear arsenals but also stem the growing ASAT threat. The first diplomatic line focused on the nuclear arms race, and resulted in a successfully negotiated arms limitations treaty, SALT II. The second, related line, was an attempt to reduce the operational ASAT imbalance. Not only were the Soviets accelerating their co-orbital ASAT tests, the US intelligence committee identified what it believed was a breakthrough in directed energy technology. A very large laser located in Sary Shagan appeared to overhead reconnaissance to have a primary anti-satellite mission (identified in the U.S. Department of Defense 1990). Since President Ford's directive to build an ASAT capability was already in place, Carter's team decided to use the DOD program as incentive to bring the Russians to the negotiating table and provide leverage once talks were under way (Stares, *Militarization*, p. 183). Both sides accused the other of developing exotic technologies and adapting treaty-allowed anti-ballistic missile systems to ASAT operations, and the talks foundered.

A fundamental change in military space policy followed with the next national election. In an effort to fulfill his campaign promise to restore American military power following its post-Vietnam malaise, defense officials in President Ronald Reagan's administration began circulating support for a fresh look at space organizational structure that would ultimately lead to a new combatant command – US Space Command. The soaring costs and inefficiencies of space systems acquisition, the mess of some 50 uncoordinated military organizations working with pieces of the space enterprise, and the threat of a Soviet program that appeared to be racing ahead in military space warfighting capabilities fueled frustrations that led to a call for action. In September 1981, the Air Force added a fifth subunit to its planning staff, the Directorate of Space Operations, to provide options. Still, as is often the case with large bureaucracies, meaningful change required a push from the outside. In late 1981, House Resolution 5130 required the US Air Force to report to Congress on the feasibility of establishing a service space command (Karas 1983; Spires, *Beyond Horizons*, pp. 188–92).

In arguments that would resurface 35 years later, the DOD strongly opposed the move on the grounds it was not needed, would duplicate bureaucracies, and cost too much. In January 1982, A GAO report undercut those arguments suggesting a separate space command that would coordinate all military space activities could instead result in overall cost savings; specialization was in fact the foundation of organizational efficiency. Thus, in June 1982, the USAF revealed it would establish a subordinate Space Command in Colorado Springs no later than September (Spires, *Beyond Horizons*, pp. 193–205). Two years after, the co-located US Space Command was inaugurated. By the end of the decade, the commander of USSPACECOM (dual-hatted as commander of the North American Aerospace Defense Command) gained authority over all military space operations, took command of land-based ballistic missile responsibilities from Strategic Air Command, secured nascent

computer operations (the precursor to today's Cyber Command) authority, inaugurated a warfighting space operations center, and created a Joint Space Intelligence Center (Ibid., pp. 217–8. Authors Note: The commander usually was commander of both US *and* Air Force Space Commands). Such rapid evolution perhaps went too far toward an independent space service and in the process threatened entrenched bureaucratic constituencies.

In 1983, President Reagan announced his Space Defense Initiative (SDI), derisively dubbed Star Wars by an incredulous press. The intent was to reverse what he believed was an immoral lack of protection for Americans. The 1972, ABM Treaty was grounded in the 1960s nuclear theory that Mutual Assured Destruction (MAD) provided by a guaranteed second strike capability was the only way to deter a nuclear exchange. The key to Reagan's approach was that missile defense would be based in space, the only deployment that had the potential to create an effective global shield against ICBMs. To comply with the national policy of peaceful intent in space, Reagan offered to share the protection of a space-based nuclear shield to all the nations of the earth, ridding the world of the only mechanism for global destruction yet devised. Whether SDI was feasible in the manner President Reagan intended, it did cause the Soviet Union to increase its missile defense and ASAT research and development, putting pressure on an economy that had essentially flat-lined, and in so doing may have accelerated its downfall. Regardless, after labeling the Soviet Union the Evil Empire, his strong approach ultimately led to a rapprochement with Soviet Premier Mikhail Gorbachev, in turn leading to the first Strategic Arms Reduction Talks (START) and a lifelong friendship between the two leaders.

The ASAT initiative begun by President Ford in 1977 finally became operational under Reagan in 1985. After two successful proof of concept tests, a modified air-to-ground HARM missile was launched from an F-15 at maximum altitude for the aircraft. The missile intercepted a defunct American scientific satellite, obliterating the target and leaving a debris cloud that remained a navigation hazard for many years. Congress quickly declared that it would no longer fund dedicated ASAT programs and the very limited US capability was set aside.

President George Bush's administration continued the general policies of his predecessors but changed the focus of the SDI program. A completely protective shield was a chimera. Moreover, the MAD doctrine appeared to be working. A guaranteed retaliation on a massive scale could deter a massive scale attack. But Bush was now more concerned with limited attack scenarios that simply could not be deterred; they could only be defended against. There were essentially four: (1) An accidental launch, (2) an irrational national leader from a rogue state that might acquire a nuclear device and use it out of malice or desperation, (3) a terrorist organization gaining control of a nuclear weapon, especially worrisome with the with the collapse of the Soviet Union, and (4) a third-party launch. If India and Pakistan were to engage in a limited nuclear exchange, or Israel and Iraq, Iran or North Korea, the result would not only be tragic, it might well draw the larger nuclear powers in. With these growing possibilities in mind, President Bush pushed ahead with a limited space defense concept developed by the SDI team called Brilliant Pebbles and Brilliant Eyes (see Dolman 2001). The system comprised a

network of some 320 satellites in low-earth orbit, each with 24 interceptors capable of engaging a satellite in the boost or intermediate phase, and a dozen reconnaissance satellites in higher orbit that could identify a missile launch from its heat signature and coordinate the best response. If it could be made operational, it was projected to be capable of engaging and destroying up to 100 simultaneous launches anywhere on earth. President William Clinton entered office in 1993 having campaigned against SDI, but was persuaded that the limited defense under Bush had merit. Instead of quickly killing the program, he gradually decreased funding so promising technologies might reach fruition. Although the system had some promising successes in early research and development, it was eventually discontinued.

Significantly, with the demise of the Soviet Union and the possibility of limited nuclear war – much less an earth-killing MAD scenario – off the minds of most Americans, Clinton’s administration reduced many of the restrictions that had kept commercial space development under wraps. Because under the OST states were liable for damaged caused to or from space activities, a commercial space launch enterprise had to be licensed by the appropriate national government. More critical in the Cold War, a private space launch could look identical to an out-of-the-blue ballistic missile attack, and the USA was loathed to give any but largest aerospace corporations that accepted continuous oversight and abided by severe restrictions on use any leeway. With nuclear war seemingly a relic of the past, restrictions were loosened under Clinton. The renaissance of private space exploration today, from corporations including Space-X, Blue Origin, and Virgin Galactic (and many smaller start-ups) would not have been possible under Cold War licensing rules.

The spectacularly successful space support debuted in Operations Desert Shield and Desert Storm prompted the Air Force to seek even greater control of the space mission. Not unnoticed, was the fact that by the mid-1990s, the space-specific portion of the DOD budget had approached \$10 billion, with upwards of 85% earmarked for the Air Force. A similar amount was distributed to government and intelligence agencies, for an average of \$18 billion annually (<https://www.af.mil/News/Article-Display/Article/113903/air-force-officials-take-space-budget-acquisition-strategy-to-capitol-hill/>). Post-Desert Storm, the US military had grown so reliant on space support that if it were denied for any reason, deployments around the world could become untenable. Former Secretary of Defense Donald Rumsfeld was tasked to lead a study of the problem. The 1998 Rumsfeld Commission Report warned of a “space Pearl Harbor” due to a lack of emphasis on space and recommended a gradual evolution toward a separate Space Corps within the Air Force as an intermediary step on the path to a separate Space Department. Unheeded, USSPACECOM authorities were steadily transferred elsewhere and any notion of a separate service was effectively dispatched. NORAD moved under the newly established North American Command and all duties not already purged were subsumed by Strategic Command. In 2002, USSPACECOM was disbanded and Air Force Space Command became the de facto US Space Force (<http://purview.dodlive.mil/2018/10/01/reestablishing-u-s-space-command/>).

None of that seemed predestined. Rumsfeld was made Secretary of Defense under President George W. Bush, and in 2001 it appeared that the most pro-military space

administration to date was going to dictate the commission's recommendations. The civilian side would be reinvigorated as well, and the slogan "Back to the Moon, and on to Mars!" was touted. The attacks of September 11, 1991 changed all that. Military funds not going to the Global War on Terror (GWOT) were pulled or substantially cut. The succeeding two wars in Afghanistan and Iraq kept focus away from space reform.

The rise of China as a major space faring nation in the twenty-first century did not go unnoticed in the USA, it was simply discounted. The first Taikonauts to go into space on Chinese rockets were a source of immense pride and were quickly followed by a series of spectacular space achievements. To Americans, the Chinese were simply doing the same things the USA had accomplished decades earlier. There was little cause for concern. In China, however, the burgeoning space program was evidence that it was finally taking its rightful place as a modern, first-tier power. In 2007, it could no longer be dismissed. China destroyed one of its aging weather satellites with a direct ascent hit-to-kill ASAT launched on a modified MRBM. The resulting debris cloud caused international outrage, an unexpected reaction as both the Soviets and Americans had done similar damage with their first ASAT tests. But now space was more congested, and much more of the global economy was enabled by space support.

While denying any connection, the USA appeared to respond to the first Chinese test the following year, destroying a deorbiting satellite with an anti-air missile launched from an Aegis cruiser, obviating any debris issues as the target was too low for fragments to remain in orbit. The USA's official position was that the incoming satellite might not burn up completely on re-entry, and its toxic hydrazine fuel could pose a danger to the environment. Regardless, it did appear to counter the Chinese demonstration with an enhanced capability of its own. The Aegis is a mobile platform that can deploy to three-fourths of the globe – a so far unmatched capability.

The official space policy of the Bush administration, while consistent with his predecessors, contained more aggressive rhetoric with regard to America's right to defend its interests in space, though action was postponed. With President Barack Obama's administration a comprehensive national space policy was issued that toned down some of the language but clearly maintained continuity with its predecessors. A more detailed exposition of the Obama NSSS follows below. American involvement in Afghanistan and Iraq, while reduced, still took up a significant portion of the nation's military budget. A globally widening threat from Violent Extremist Organizations (VEOs), most notably the Islamic State of Iraq and Syria (ISIS), and a slow recovery from the profound recession caused by the 2007 collapse of the US housing crisis meant military space priorities remained on the back burner.

China's space capabilities accelerated, and Russia's resurfaced. In 2017, an exasperated Mike Rogers (R-AL), Chair of the House Armed Services Strategic Forces Subcommittee, concerned that America now faced multiple near-peer competitors in outer space had enough. Implicitly accusing the USAF of diverting space funds to priority air projects, and mismanagement of the rest, Rogers and representative Jim Cooper (D-TN) inserted language into the 2018 National Defense

Authorization Act (NDAA) directing an independent Space Corps in the Air Force along the lines of the Marine Corps in the Navy (<https://spacenews.com/congress-man-rogers-a-space-corps-is-inevitable/>). The measure passed the House but was tabled in the Senate pending further study. The Air Force pushed back strongly and marshalled precisely the same arguments the US Army used in its attempts to retain the US Army Air Forces after WW II; it wasn't needed as the purpose of the air arm was to support the fight on the land (and therefore was best overseen and coordinated by the land commander), it would create an unnecessary parallel bureaucracy, and therefore be too expensive. Demonstrating an astonishing lack of historical acumen, the Air Force argued that an independent separate space corps would take away from its primary mission in support of terrestrial forces, it would create an unnecessary parallel bureaucracy, and therefore be too expensive.

Although the president's administration staunchly opposed Rogers' and Cooper's plan, after the mid-term elections President Trump one-upped the Space Corps blueprint and surprisingly announced his intention to create a separate and equal Department of the Space Force. In June of 2018, Vice President Pence detailed the administration's vision (<https://www.nbcnews.com/politics/white-house/trump-says-he-directinh-pentagon-create-new-military-branch-called-n884361>). The USAF would immediately begin comprehensive preparations to split off a co-equal Department of the Space Force including a US Marine-style independent organizational structure within the Department of the Air Force. It would draft a plan for congressional budget support, and coordinate with other services and national intelligence space cadres for efficiencies.

Publicly supporting the initiative, USAF leadership continued to privately argue the folly of the move. It would be bureaucratically redundant and wastefully expensive. A memo from the Office of the Secretary of the Air Force was released (or "leaked"; <https://www.defenseone.com/politics/2018/09/creating-space-force-will-cost-13b-ove-5-years-air-force-secretary/151312/>) stating a 5-year conservative estimate of the additional cost of separating an independent space service would approach \$13 billion over 5 years, "likely to be revised upward" (<https://spacenews.com/wilson-13-billion-space-force-cost-estimate-is-conservative>).

By October, however, Air Force leadership appeared to have dropped even veiled opposition, and submitted a viable, comprehensive transition plan for congressional approval at the end of February 2019. Surprisingly, the anticipated cost of the transition would be quite low, and bureaucratic overlap remarkably lean. The Pentagon requested just \$72 million for fiscal 2020 and just \$2 billion over the next 5 years to stand up a functioning Space Force within the Department of the Air Force (<https://insidedefense.com/daily-news/pentagon-estimates-new-space-force-will-cost-2-billion-over-five-years>). Beginning with less than 200 assigned personnel in the first year, the Space Force should grow to approximately 15,000 military and civilian billets by 2025. After that, when the organization is expected to be fully operational, the Pentagon's plan would stabilize the Space Force budget at about \$500 million per year, or "about 0.07 percent of the Defense Department's annual budget" (<https://abcnews.go.com/Politics/join-space-force-academy/story?id=61411343>).

## Current US Space Policy

The National Security Space Strategy (NSSS) is subordinate to the National Space Policy (NSP), which outlines and defines the overall direction and emphases of America's space programs. The most recent published NSP was issued under the Obama administration in 2010. It describes an increasingly diverse space environment but is more representative of a continuation of the rhetoric and substance of the preceding Bush and Clinton administration policies than a "bold new course" (National Space Policy of the United States of America 2010). The future impetus for space development shall emphasize a more international focus, as humanities' reliance on space for an increasingly interconnected global network of finance, trade, production, and security has changed the way we live, "and life on Earth is far better as a result" (Ibid.).

Until the details of the Trump NSSS and NSP are released, guidance for space planning and organizational described in the Obama NSP technically remains in effect. It is not expected that the logic of that document will be completely discarded, and so potentially relevant portions are summarized here as still-current policy. Where the present and previous administrations are not reconcilable is in their underlying premises. President Obama declared the old narrative of national space development, born of conflict and propelled by Cold War challenges, must give way to a new era of cooperation. It called for a renewed commitment to international harmony, the rights of all nations to pursue the peaceful exploration and use of space, and the continuing leadership role of the US in these efforts. But "in this spirit of cooperation," within the five guiding principles put forth for all states to adopt and follow, is the recognition that among the peaceful purposes advocated therein the right of the United States to use space "for national and homeland security activities [and] consistent with the inherent right of self-defense, [to] deter others from interference and attack, defend our space systems and contribute to the defense of allied space systems, and, if deterrence fails, defeat efforts to attack them" is maintained (Ibid., 3). Accordingly, the Secretary of Defense is charged with the development, acquisition, operation, maintenance, and modernization of Space Situational Awareness (SSA) capabilities; Developing capabilities, plans, and options to deter, defend against, and, if necessary, defeat efforts to interfere with or attack USA or allied space systems; Maintaining the capabilities to execute the space support, force enhancement, space control, and force application missions; and Provide, as launch agent for both the defense and intelligence sectors, reliable, affordable, and timely space access for national security purposes (Ibid., 14).

Consistent with 2010 NSP, the Department of Defense published the 2011 National Space Security Strategy. This document "charts a path for the next decade to respond to the current and projected space strategic environment" (Ibid., i). That environment, state the authors, is driven by three trends; "space is becoming increasingly *congested*, *contested*, and *competitive*" (Ibid., 1. Original emphasis). *Congestion* here refers to the increasing clutter in space, primarily in low-Earth orbit, that has come as a natural result of space launches, satellite deployments, and, not so

naturally, from anti-satellite weapons testing. The DOD tracks more than 22,000 objects in orbit that are large enough to be detected by ground sensors, including more than 1,200 active satellites, to assist in payload identification and collision avoidance. Potentially hundreds of thousands of smaller objects also exist in orbit, where the kinetic impact of a pin-head size bit of metal or ceramic could destroy a satellite or puncture a space-suit. In recent years, two events have significantly increased the size of the debris field; a 2007 Chinese ASAT test that obliterated one of its own derelict weather satellites added approximately 3,000 trackable chunks of debris and the 2009 collision of a Russian Cosmos and an American Iridium satellite, resulting in 1,500 additional pieces of observable debris (Ibid., 2). Not only is this effective physical pollution of LEO expanding exponentially, the useable radiofrequency spectrum is increasingly stressed, causing frequent unintentional interference between satellites and reducing bandwidth carrying capability.

Space is also increasingly *contested*. “Today space systems and their supporting infrastructure face a range of man-made threats that may deny, degrade, deceive, disrupt, or destroy assets. Potential adversaries are seeking to exploit perceived space vulnerabilities” (Ibid., 3). The emphasis here is on direct military intervention against US space assets that disrupt the stability and security of the space environment, though it includes unintentional interference through so-called irresponsible behavior.

*Competition* refers to the declining relative edge in space capabilities held by the USA. The NSSS maintains that America’s competitive advantage in space access and market share is dissipating, and its lead in space technology is eroding as more states enter into the strategic environment. Limited access to space is challenging America’s “abilities to maintain assured access to critical technologies, avoid critical dependencies, inspire innovation, and maintain leadership advantages. All of these issues are compounded by challenges in recruiting, developing, and retaining a technical workforce” (Ibid.).

The December 2017 National Security Strategy formalized an abrupt shift in emphasis. In his introduction, President Trump opens with the statement “[T]he American people elected me to make America great again” (<https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>, p. i). He concludes, “This National Security Strategy puts America First” (Ibid., p. ii). The NSP highlights “the growing political, economic, and military competitions we face around the world” and specifically charges China’s and Russia’s efforts “to erode American security and prosperity” (Ibid., p. 2). Asserting: “An America that successfully competes is the best way to prevent conflict. Just as American weakness invites challenge, American strength and confidence deters war and promotes peace” (Ibid., p. 3). The NSS details four “vital national interests” that undergird the America First strategy (Ibid., pp. 3–4):

- First, our fundamental responsibility is to protect the American people, the homeland, and the American way of life.
- Second, we will promote American prosperity.

- Third, we will preserve peace through strength by rebuilding our military so that it remains preeminent, deters our adversaries, and if necessary, is able to fight and win.
- Fourth, we will advance American influence because a world that supports American interests and reflects our values makes America more secure and prosperous.

The entire section on space, upon which the National Space Policy is presumably based, is less than one page. Following a review of increasing competition in space, and insistence that the US “must maintain our leadership and freedom of action in space,” the section concludes that “any harmful interference with or an attack upon critical components of our space architecture that directly affects this vital U.S. interest will be met with a deliberate response at a time, place, manner, and domain of our choosing” (Ibid., p. 31).

Four months later, on 23 March 2018, President Trump’s White House announced a new National Space Policy to replace the 2011 Obama administration NSP, opening with the statement: “AMERICA FIRST AMONG THE STARS: President Trump’s National Space Strategy works within his broader national security policy by putting America’s interests first” (<https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy/>). While the full text of the strategy has not been released, the announcement assures that the new strategy “prioritizes American interests first and foremost, ensuring a strategy that will make America strong, competitive, and great” (Ibid.). Accordingly, the NSP promises to maximize cooperation between the military, civil, and commercial space sectors, to include prioritizing “regulatory reforms that will unshackle American industry” (Ibid.). In further challenging almost six decades of cooperative rhetoric that recognizes space as the common heritage of humankind and that its benefits should be shared equally among all nations and people, “[t]he new strategy ensures that international agreements put the interests of American people, workers, and businesses first” (Ibid.).

The announced NSP was followed by four Space Policy Directives (SPDs):

- SPD-1 (11 December 2017) directs NASA to “lead the return of humans to the Moon for long-term exploration and utilization, followed by human missions to Mars and other destinations,” instead of an asteroid as the Obama Administration planned (<https://spacepolicyonline.com/topics/militarynational-security-space-activities/>; <https://www.whitehouse.gov/presidential-actions/presidential-memo-random-reinvigorating-americas-human-space-exploration-program/>).
- SPD-2 (23 March 2018) “Streamlining Regulations on Commercial Use of Space,” directs the Secretary of Transportation to investigate and minimize requirements levied on commercial space activities and licensing of commercial launch and re-entry activities (<https://www.whitehouse.gov/presidential-actions/space-policy-directive-2-streamlining-regulations-commercial-use-space/>).
- SPD-3 (24 May 2018) “National Space Traffic Management Policy,” uses the language of the Obama NSP (space is “congested and contested”) to direct steps



to improve SSA and mitigate the effects of orbital debris (<https://www.whitehouse.gov/presidential-actions/space-policy-directive-3-national-space-traffic-management-policy/>).

- SPD-4 (14 February 2019) specifies the transition plan for creating a military space force (<https://www.whitehouse.gov/presidential-actions/text-space-policy-directive-4-establishment-united-states-space-force/>).

SPD-4 was released with a full DOD-produced brochure titled “United States Space Force” (<https://media.defense.gov/2019/Mar/01/2002095012/-1/-1/1/UNITED-STATES-SPACE-FORCE-STRATEGIC-OVERVIEW.PDF>). It is the most far-reaching initiative in military space organization to date, though it is substantially less radical than President Trump’s stated intention to establish a *separate Department* of the Space Force, co-equal to the Army, Navy, and Air Force. The brochure was accompanied by a detailed formal reorganization plan for congressional approval establishing Title XII authority for a US Space Force (<https://media.defense.gov/2019/Mar/01/2002095010/-1/-1/1/UNITED-STATES-SPACE-FORCE-LEGISLATIVE-PROPOSAL.PDF>). The plan will likely go through several revisions before passage, but the key points from all three documents should remain essentially intact.

The Space Force will become the sixth formal branch of the US military, housed within the Department of the Air Force, responsible for Organizing, Equipping, and Training (OTE) all space forces, by fiscal year 2020. A unified combatant command, the United States Space Command, shall also be established, and will be responsible for Joint Force space operations. These organizations will “provide for freedom of operation in, from, and to the space domain; ... provide independent military options for national leadership ... both combat and combat support ... to enhance the lethality and the effectiveness of the space domain” (<https://www.whitehouse.gov/presidential-actions/text-space-policy-directive-4-establishment-united-states-space-force/>).

---

## Conclusion

The world economy is so intrinsically linked to support from space that should a major outage of satellite capacity occur, financial and trade markets could collapse. A recession spanning the globe would ensue, and security tensions would exacerbate. The increasingly chaotic international environment would be further destabilized by the disastrous incapacitation of US military power. Without the assuredness of space-based surveillance, communications, and navigation support, American and allied military forces would be ordered to hunker down in defensive crouch while preparing to withdraw from dozens of then-untenable foreign deployments.

Such a scenario is not only possible – given the growing investment and reliance on space as a national power enabler – it is increasingly plausible. An attack against low-Earth orbit from a medium range ballistic missile adapted for detonation in space could cause inestimable harm to the national interests of developed and

developing states alike. Deterrence may forestall such an attack, but without a space-based defense any decision by an adversary to disrupt space capabilities on-orbit is likely to succeed. The US leadership now believes that it is irresponsible to rely on the better intentions of its adversaries, international agreements, and deterrent threats to guarantee its national space interests. The shift in American space policy makes clear that space is now considered a warfighting domain, and the USA will prepare itself to fight and win military conflicts that might occur there. How the world reacts will ultimately determine the wisdom of these decisions.

---

## References

- Baker D (ed) (2005) Jane's spaceflight directory 2004–2005. Jane's Information Group, Alexandria, pp 611–612
- Christopher Preble (2004) John F. Kennedy and the missile gap. Northern Illinois University Press, DeKalb
- Dolman E (2001) *Astropolitik: classical geopolitics in the space age*. Frank Cass, London, p 47
- Futrell R (1985) Ideas, concepts, doctrine: basic thinking in the United States Air Force 1907–1960, vol I. Air University Press, Maxwell AFB, p 550. [https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B\\_0032\\_FUTRELL\\_IDEAS\\_CONCEPTS\\_DOCTRINE.pdf](https://www.airuniversity.af.edu/Portals/10/AUPress/Books/B_0032_FUTRELL_IDEAS_CONCEPTS_DOCTRINE.pdf)
- Houchin R (2006) US hypersonic Research and Development: the rise and fall of dyna-soar, 1944–1963. Routledge, New York
- Johnson-Freese J (2007) Space as a strategic asset. Columbia University Press, New York, p 44
- Johnson-Freese J (2009) *Heavenly ambitions: America's quest to dominate space*. University of Pennsylvania Press, Philadelphia, p 35
- Karas T (1983) The new high ground. Simon & Schuster, New York, pp 17–20
- Mieczkowski Y (2013) Eisenhower's sputnik moment: the race for space and world prestige. Cornell University Press, Ithaca, pp 78–79
- Mowthorpe M (2004) The militarization and Weaponization of space. Lexington, Lanham, p 58
- National Security Space Strategy*, Unclassified Summary, January (2011). [http://www.defense.gov/home/features/2011/0111\\_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary\\_Jan2011.pdf](http://www.defense.gov/home/features/2011/0111_nsss/docs/NationalSecuritySpaceStrategyUnclassifiedSummary_Jan2011.pdf)
- National Space Policy of the United States of America*, 28 June 2010, p. 1. [http://www.whitehouse.gov/sites/default/files/national\\_space\\_policy\\_6-28-10.pdf](http://www.whitehouse.gov/sites/default/files/national_space_policy_6-28-10.pdf)
- Neufeld M (2007) Von Braun: Dreamer of Space, Engineer of War. Vintage, New York, ch. 9
- Plait P (2019) The 50th Anniversary of Starfish Prime: The Nuke that Shook the World. Online at <http://blogs.discovermagazine.com/badastronomy/2012/07/09/the-50th-anniversary-of-starfish-prime-the-nuke-that-shook-the-world/>
- RAND (1946) Preliminary Design of an Experimental World-Circling Spaceship. RAND, Santa Monica. [https://www.rand.org/pubs/special\\_memoranda/SM11827.html](https://www.rand.org/pubs/special_memoranda/SM11827.html)
- Sheehan N (2010) *A fiery peace in a cold war: Bernard Schriever and the ultimate weapon*. Vintage, New York
- Spires D (1998) *Beyond horizons: a half century of air force space leadership*, revised edn. Air University Press, Maxwell AFB, p 9
- Stares P (1985) *The militarization of space: U.S. policy 1945–84*. Cornell University Press, Ithaca, pp 41–43
- U.S. Department of Defense annual publication. *Soviet Military Power*. September 1990, pp 60–61
- Ware W (2008) *RAND and the information evolution: a history in essays and vignettes*. RAND, Santa Monica, p 6
- Zak A (November 16, 2015) Here is the Soviet Union's Secret Space Cannon. *Popular Mechanics* <https://www.popularmechanics.com/military/weapons/a18187/here-is-the-soviet-unions-secret-space-cannon/>



Nicole J. Jackson

## Contents

Introduction .....	386
Russia's Space Security Policy: Consistency and Change .....	387
Context .....	387
Russia's Perceptions of Space: Threats and Opportunities .....	388
Russia's Space Diplomacy .....	395
Conclusion .....	397
References .....	398

## Abstract

Russia's outer space policies fit within its domestic and foreign policy efforts which focus on asserting Russia's authority, status, and prestige and reviving its economy. Outer space has also become an important area through which Russia aims to respond to Western strategy and capabilities and also influence global norms. Military efforts are but one part of a complex set of tools, employed to navigate what Russia perceives as an increasingly hostile world. Its economic, military, and technological weaknesses compared to the USA and NATO have led Russia to pursue asymmetric tactics which include working through bilateral bodies and those affiliated through the UN on space policy. These give it publicity and some legitimacy but little ability to make significant progress on the substantive issues.

---

N. J. Jackson (✉)

School for International Studies, Simon Fraser University, Vancouver, BC, Canada

e-mail: [nicole\\_jackson@sfu.ca](mailto:nicole_jackson@sfu.ca)

## Introduction

Outer space security may be viewed through a national security (or “militarization of space”) approach which focuses on the use of space-based technology to protect against outside threats; from a “peace approach” centered, for example, on using technology for arms control verification, humanitarian relief, and climate change; or from a “security in outer space” approach concerned with how to prevent overcrowding, debris in space, and conflicts over space resources.

Today, the Russian Federation is a major actor in space, and Russia’s outer space policy encompasses all three approaches. In this chapter, I focus primarily on Russia’s national strategic security and outer space governance. Russia-US international space cooperation, for example, on the International Space Station and their scientific cooperation in the exploration of space, is beyond the scope of the chapter.

Russia considers outer space predominantly as a strategic region to enhance its military capabilities on Earth, provide intelligence and communication functions, and achieve international status and prestige as a space power. It is reactive to US strategy and actions and has developed counterspace technologies (e.g., electronic weapons that can jam satellites) to provide Russia with an asymmetric edge to offset US military advantages. However, Russia’s outer space rhetoric and policy are also driven by domestic and identity issues. Outer space strategy is an instrument through which Russia pursues its goal to be a “great power” and to mold the international system more closely to a new multipolar world as it sees it. It could also bring Russia economic benefits while masking internal challenges.

President Vladimir Putin has taken both symmetric and asymmetric actions in outer space. He has increased Russia’s investment in new technologies (satellites, electronic warfare, strategic offensive weapons, etc.) and simultaneously pursued diplomatic initiatives to control weapons in space. During the Cold War, despite military tensions and serious concern about a possible arms race in outer space, Russia and the USA negotiated internationally binding agreements related to the governance of space activities. Today, both powers are again a warning of a new arms race in outer space while continuing to strengthen their military capacities in the field.

Since 2000 Russia has actively pursued both binding laws and non-binding norms to ban and control weapons in outer space and has advocated for non-binding, voluntary transparency and confidence-building measures (TCBMs). Sometimes it has done this in cooperation with other states, sometimes in opposition to them. This diplomatic endeavor may seem somewhat at odds with Russia’s growing militarization; however, their dual role on outer space fits well within Russia’s overall foreign and security strategy which is reactive to US policy and simultaneously pro the United Nations (UN) and consensus-based multilateral negotiations. Russia is strengthening its comprehensive power, including military, diplomatic, and normative global influence, in order to make its voice heard on the international stage. Russia’s diplomatic activism is that of an aspirational great power, but it also reflects the limits of its current economic and military capabilities. International negotiations enable Russia to be recognized as a key player in global

affairs while also benefiting from an opportunity to highlight the US/West's declining influence and the rise of a multipolar world.

This chapter examines why outer space is so important for Russia. Then, it shows how and why the Russian government's outer space policy, strategy, and capabilities have evolved since the Soviet Union collapsed. The paper concludes with an appraisal of Russia's recent diplomatic initiatives in the field of outer space governance. No longer economically competitive in the race for control of outer space, Russia has attempted several strategies to enable it at least to keep in the running. It has placed its space strategy in the context of defense requirements and state military control. It is using diplomacy – working with international organizations affiliated with the UN – to discuss, cooperate on, and influence the race for the militarization of space. It works with disarmament organizations to influence and promote a collective approach to the problem, rather than one dominated by the richer and more powerful states.

---

## **Russia's Space Security Policy: Consistency and Change**

### **Context**

Russia's outer space policy should be viewed in the context of the many significant and complex challenges of keeping outer space "secure." For example, there is a growing number of active spacecraft in orbit and well over a thousand satellites operated by more than 70 states and commercial and civil entities. Militaries increasingly rely on space operations and on long-range satellite communications and data transfers to train, navigate, and operate. Satellites and space-based servers are also increasingly important to everyday life. Banking, communications, transportation, and the Internet are all dependent on access to space, as are weather prediction, natural disaster mitigation, and sustainable farming. In sum, space-based infrastructure weaves together the world economy.

At the same time, with globalization and the changing global balance of power, the numbers, diversity, and interdependencies of state and non-state actors involved in outer space are growing. Rapid technological changes provide ever greater access to space. Space has also moved to the forefront of the global security debates because of renewed attention to kinetic anti-satellite (ASAT) capabilities and other non-kinetic denial capabilities, e.g., jammers and lasers. The situation is becoming ever more complex with the evolving role of cyber and artificial intelligence (AI) and growing mistrust between actors. This adds urgency and new challenges to the development of Russian (and other actors') outer space security policy and to multilateral approaches to space governance.

Russia today is second only to the USA as a major space actor. However, many state and non-state actors are increasingly interested in the benefits and threats of outer space and have increased their space capabilities. Each has its own evolving perceptions and priorities. The USA has the largest space budget, a large network of military and commercial satellites, and a growing commercial space sector. China

has developed a multifaceted space program. The EU is increasingly investing in its space program and has sought to negotiate an international code of conduct.

There has also been an explosion of commercial space actors who have very specific priorities such as would-be asteroid mining ventures or small satellite operations. And there is a growing competition for access to the most useful parts of the radio-frequency spectrum for satellite operations. Commercial actors are challenging and pushing the boundaries of traditional governance regimes and old Cold War frameworks. They are thus forcing states to rethink regulatory and legal regimes. At the same time, individuals and knowledge institutes now have access to space thanks to decreasing costs of increasingly small satellites (micro, mini, nano).

So far, the dominant powers have shown a significant degree of restraint in their activities. And most states continue to maintain that an arms race in outer space should be prevented, including in annual resolutions adopted by the UN General Assembly. However, this state of affairs is being jeopardized by the ongoing competition between major state actors. Recent assertions that outer space is becoming another “war-fighting domain” have been made by China, Russia, the USA, France, the UK, NATO, and India. Outer space has already been militarized but not weaponized, with passive military use being accepted under a broad understanding of “peaceful purposes” of the Outer Space Treaty of 1967. Today, many militaries, not just Russia’s, have indicated a desire for defensive and even offensive space-based capabilities. Many militaries have also initiated efforts to create dedicated military units for space including Russia, the UK, the USA, China, France, India, and Japan.

## **Russia’s Perceptions of Space: Threats and Opportunities**

The Russian state defines threats largely in traditional terms of territorial protection from military challenges and views space assets as vital for military communication and defense. Russia’s geography highlights the need to protect its extensive borders and military and economic assets and infrastructure scattered over its vast territory. The state has traditionally assessed that it is surrounded by hostile powers and thus needs “buffers” or a “sphere of influence” to protect itself. Today, Russia has expanded this rhetoric of vulnerability to include attacks from outer space. Russians use the term “aerospace” rather than outer space because of the interrelatedness of air space and outer space in the context of contemporary threats and conflicts and because there is no distinct boundary between the two concepts. Russia’s rhetoric on outer space broadly mirrors that of the USA, stressing urgency to prepare for a possible future war there.

Rapid technological advancements in the space industry have influenced perceptions that there are economic benefits from being a space power. At the same time, they have given rise to concerns about threats stemming from the militarization of space. For example, the development of cheap miniature satellites promises speedy replacement of disabled satellites in the event of attack. Theoretically, this could allow the US military (or other actors) to use such space constellations to support

operations during a conflict. Through technology outer space has become integrated with other domains – land, sea, air, and cyber. Most recently, the first generation of hypersonic weapons has “set the conditions for the merger of air and missiles defense and the air and outer space domains” (Charron and Fergusson 2018). Of course, a healthy space industry also provides strategic resources for a state’s military and economy. In Russia’s case, the announcement of new technological developments also masks unaddressed structural and systemic weaknesses and confers domestic and international legitimacy on Russia’s aspiration to be a “great power.”

Russia’s official perceptions today are not very different from those of the Soviet period. Outer space has long been significant to Russia, and now it again has the resources to be a major contender. Under Putin, as in Soviet times, Russia seeks global strategic parity with the USA and securitizes the US threat to its nuclear deterrence. Russia perceives a US first strike against its nuclear forces from space-based weapons as the key security threat from space. Its 2010 and 2014 military doctrines classify both the deployment of strategic missile defenses (the intention to place weapons in space) and the deployment of strategic conventional precision weapons as key military dangers to Russia. Other threats listed include impeding state command and control and disruption of strategic nuclear forces, missile early warning systems, and systems for monitoring outer space. Both these doctrines and the 2016 Foreign Policy Concept highlight the USA and NATO as potential enemies at a time of “increased global competition” and conclude that Russia needs to focus on the credibility of its nuclear deterrent but also on conventional and non-conventional elements in a complex toolkit of responses.

Russia has also adamantly opposed US plans for ballistic missile defense (BMD), which it perceives as opening a door toward space-based weapons integrated into BMD architecture and in turn could threaten Russia’s strategic missiles forces. The 2002 US withdrawal from the 1972 Anti-Ballistic Missile (ABM) Treaty paved the way for deployment of intercept missiles, and Russians interpreted this move as undermining the consensus on the strictly peaceful use of space. In this context, in 2015 Russia has threatened that “any action undermining strategic stability will inevitably result in counter measures” (Russian Government 2015). Russia’s key security preoccupation has been the prospect of space-based interceptors and the US refusal to accept constraints on BMD. It continues to denounce the US withdrawal from the ABM Treaty and argues that the development of US ground- and sea-based missile defense has increased tensions and led to increased missile proliferation which Russia directly links to space-based threats.

The Russian (and Chinese) governments also believe that their missiles and satellites are targeted by US antimissiles, and there is a similar assessment from the USA about Russia. Russia perceives anti-satellite weapon tests (ASATs) by China (2007), the USA (2008), and India (2019) to be precursors to the weaponization of space. ASAT capabilities are those that target an adversary’s satellites with the intention of disabling their function – communications; intelligence, surveillance, and reconnaissance (ISR); and positioning, navigation, and timing (PNT) – through interference or damaging/destroying the satellite entirely. The latter creates a second-

order effect of creating space debris that threaten other space assets and activities in that spatial region. These trends blur the traditional divide between peaceful purposes and warfare, thus making them challenging for governance and arms control.

The Russian government argues that these multiple developments are leading to a new arms race that disrupts broader arms control and disarmament processes and requires Russia's huge expenses for its space program. In March 2018 Putin announced the development of some 300 new "strategic weapons" which he said was a response to US missile defense capabilities and then unveiled several at the annual Victory Day military parade. (The West is particularly concerned about new anti-access/area-denial (A2/AD) capabilities (air and missile defenses; surface-to-surface ballistic missiles; land-, air-, and sea-launched cruise missile batteries; layered anti-submarine capabilities).) Such showmanship was not new, but Putin's hyperbole and critique of the West have intensified, and Western concern about Russia's intentions and growing, if overblown, capabilities is likely to continue.

### **1990s: A Period of Retrenchment, Decline, and Dependency**

The Soviet Union was a pioneer and military superpower in outer space. Russia inherited the Soviet Union's strategic and tactical nuclear forces. What is more, Russia continues to view its nuclear forces as an equalizer to US power and a way to preserve its great power standing. However, following the Soviet collapse, there was a dramatic decrease in Russia's space budgets, and Russia failed to maintain most of its space assets. Its space industrial complex suffered greatly, and subsequent attempts to rebuild it encountered many structural and budgetary weaknesses. Nevertheless, Russia also inherited unique capabilities (such as early warning satellites) which are vital as the main guarantee for its state security that continued (and continues) to be based on nuclear deterrence.

The 1990s in Russia were characterized overall by economic stagnation, military disintegration, and dependency on the West. It lost not only most of the military capabilities it had in space but also its ability to conduct long-term research and development. In this context, official rhetoric at the time prioritized defensive operations, as it had under Gorbachev.

Russia did continue to exercise full jurisdiction and control over space objects launched earlier by the USSR. However, it lost some infrastructure for satellite control and space surveillance (a crucial part of its early warning system). Losses included stations used to control and receive data from civilian and military spacecraft which were scattered across Russia and also in Ukraine, Kazakhstan, and Uzbekistan. Many of its radar stations also were located outside Russia's territory, and in the 1990s, Russia had to rely on older radars and negotiate the use of alternative stations outside Russia (in Azerbaijan, Belarus, Kazakhstan, Ukraine). Russia also had to rely on Western joint ventures to commercialize its launchers, its combat aircraft used US satellite navigation system, and its Northern Fleet relied on data from Canada's Radarsat-1 satellite.

During the Cold War, the Soviet Union had developed and tested ASATs in the 1960s and 1970s, before it announced a moratorium on testing in 1983. In 1993, Yeltsin continued this policy and warned that any measure to weaponize space



would be reciprocated. Russia kept dormant its technological capabilities to develop and operate terrestrial ASAT weapons (Venet 2015). The Soviet satellite navigation system GLONASS (Global Navigation Satellite System) had launched in 1982 for military purposes as counterpart to US GPS (Global Positioning System). This preparation for war included a huge number of low-quality satellites and anti-satellite systems. In the 1990s, however, Russia was unable to keep enough satellites in orbit. Its early warning and "Earth observation" systems were significantly degraded, and it suffered many challenges including lack of funding, short life of satellites, and launch problems.

Russia's 1993 law "On Space Activity" aimed to create a normative legal base to regulate space. It states that Russia shall promote the development of international cooperation in the field of space activity, as well as the solution of international legal problems that may arise in the exploration and use of outer space. It lists the key bodies in charge of space activity – the Supreme Soviet (ratifies international treaties on space activity, adopts legislation about space activities, etc.); the president (issues edicts and executive orders); government (supervises state activities and the Federal Space Program proposed by the Ministry of Defense); the Russian Space Agency (Roscosmos), and the Russian Academy of Sciences.

### **2000–2008: Russia's Securitization and Militarization of Space**

The Russian economic recovery in the 2000s coincided with a political emphasis on space as a strategic sector and subsequent increases in its state budget. Space became a symbol of Russia's revived international standing, and attempts were made to restore its former space glory and prestige. For Putin, space policies became a central tool in Russia's rebirth as a great power and its drive for independence from the West, and he prioritized rebuilding and modernizing Russia's military space capabilities. Clearly, he aimed to reduce Russia's dependencies on West (especially on technology and military data) and ensure strategic autonomy and independent access to space.

Russia began restructuring its space industry in the early 2000s, increasing the role of the state (as it did in other strategic sectors). Space and defense industries reoriented production away from export markets toward national armed forces. Both sectors were placed under the new Military-Industrial Commission (Voenno-promychnennaia komissiiia (VPK)). Venet writes that this led to mixed results, including some "spectacular failures," e.g., the loss of military and dual-use satellites, foreshadowing President Medvedev's call for more extensive military reforms (Venet 2015, p. 360). Russia's policies on space militarization (use of space assets to support military actions on Earth) continued to focus on the territory of Russia and the former Soviet Union. According to Venet, Russia could not return to the Soviet global approach (i.e., maintain the "high number of military launches and... extensive constellations of military spacecraft needed for all for military communications, navigation, surveillance, early warning, signals intelligence etc.") (Venet 2015, p. 363).

During Putin's first two terms, many state programs and presidential decrees brought Russia into a leading position in the space industry, developed new public-

private partnerships, and expanded international cooperation. (These included three major space policy documents: Federal Space Program (FSP) (2005–2015); Federal Program on Global Navigation Systems (GLONASS) for 2002–2011; Federal Special Program for the Development of Russia’s Cosmodromes (DRC) for 2006–2015; and Federal Target Program for GLONASS development 2013–2020.) However, even with steady economic growth during these years, space spending remained precarious, prompting Roscosmos (the Federal Space Agency) to petition President Putin for more funding. In the early 2000s, GLONASS was revived and new satellites were launched. This provided a source of prestige and a symbol of independence from the USA in positioning, timing, information, and navigation.

Concurrently, Russia began to modernize its ground infrastructure (important for satellite control, space surveillance networks, and cosmodromes). It brought ground-based assets back to the Russian territory and militarized space assets already there. For example, Roscosmos took over the Baikonur Cosmodrome in Kazakhstan, and the Plesetsk Cosmodrome in Northern Russia was set to become Russia’s major military spaceport. Russia also revived its ASAT system program (not co-orbital ASAT system) and made substantial advances in ballistic missiles, radars, and missile defense interceptors (details below).

### **2008–2013: Halting Modernization and Growing Ambitions Following the Russia-Georgia Conflict**

After Russia’s war in Georgia in 2008, and with President Medvedev in power, the push for space modernization resumed, although uncertainty over funding and overambitious plans continued. Russia’s space industry did survive the 2008 world economic crisis, declining oil revenues, and foreign capital flight thanks to government subsidies. However, the war in Georgia highlighted the limits of Russia’s military capabilities and the failure of its command and control system. Space-based intelligence was deficient, and satellite communications facilities were not useable. There was no situational awareness, and satellite targeting was not operational (for artillery or precision-guided munitions).

Russia’s early warning system (crucial for nuclear deterrence) improved in subsequent years but still lacked global detection. Then, it lost its last major satellites in 2014. GLONASS regained full operational capacity only in December 2011 when the second-generation GLONASS-MA entered service, but difficulties with the technology and political disputes over its deployment lingered. However, there is evidence that the Russian government during these years increasingly perceived space-based systems as highly important and essential for integration of command, control, communications, information, surveillance, and reconnaissance (C3ISR) and also for what Russians call the “information-strike operations” – which consist of “information-strike battles, information-weapons engagements and strikes with the goal of disrupting enemy troop command and control of weapons systems and the destruction of its information resource” (Johnson-Freese 2017, p. 44).

The 2011 Presidential Decree on science and technology, which provides the current legal basis for technological development of the Russian economy, included

plans for space, information, and communications systems (President of the Russian Federation 2011). However, many of the projected missions and launches were postponed, and a gap between stated goals (e.g., creation of a unified, information, command, and control system) and realities remains. Many experts question the quality of Russia's space-based communication system as well as the required infrastructure on the ground. As a result, it has often been suggested that the Russian armed forces did not evolve relative to new combat realities and that Russia should focus more on reconnaissance, electronic warfare capabilities, command and control, data processing, and information distribution systems (Gareyev 2009; McDermott 2012; Roffey 2013).

### **2014 and Beyond: Moving to the Offensive?**

Since Russia's annexation of Crimea in 2014 and its military involvement in Syria, tensions between Russia and the West have increased dramatically. Russia's 2014 military doctrine included in its list of key external threats: "global strike," the intention to station weapons in space, and strategic non-nuclear precision weapons (Russia's Security Council 2014). (Prompt Global Strike is the Pentagon's strategy of being able to strike anywhere in the world with a conventional warhead in less than an hour.) Russia continues to argue that to preserve the strategic balance of power it must respond to US actions. It therefore seeks to limit the technical superiority of the USA by focusing on counterspace activities such as cyber and electronic warfare while fostering uncertainty about its own intentions. The potential threat to Russia's strategic nuclear deterrent and the US pursuit of "global strike" conventional precision missile systems are frequently cited as the main reasons that "Russia can't consider further reductions of offensive forces at this time." Overall, while Russian rhetoric has become increasingly bellicose, Russia continues to militarize and centralize its policies on outer space with an emphasis on the importance of information. The stated strategic priorities of its current Security Strategy include "Strengthening the country's defense, ensuring the inviolability of the Russian Federation's constitutional order, sovereignty, independence and national and territory integrity" and 'consolidating the Russian Federation's status as a leading world power, whose actions are aimed at maintaining strategic stability and mutually beneficial partnerships in a polycentric world" (The National Security Strategy of the Russian Federation 2015).

Some argue that a close reading of Russia's current space documents reveals confusion about different goals and budgets (Zak 2018). However, the documents also reveal Russia's key principles on space policy, including the protection of state interests such as the right to self-defense; the promotion of economic development, including the development of space assets, launch vehicles, and ground infrastructure; the development and use of space technology and goods and services in the interests of Russia's socioeconomic sphere and the space and rocket industry; and maintenance of Russia's primary position in piloted flights. Public documents include plans to create a new generation of space complexes and systems to be competitive in the world market and, once again, the completion of the GLONASS system.

The Federal Space Program, a long-term planning document (Space Activity of Russia in 2013–2020, 2014) listed three goals: contributing to the development of the economy; enhancing national security and strengthening Russia's position in the world; and increasing the welfare of Russia citizens [my bold]. The subsequent Federal Space Program 2016–2025 continues to prioritize the competitiveness and large-scale use of the GLONASS system as well as ground infrastructure for space activities.

Since 2014 the centralization of Russia's space industry has advanced. It reverted to state ownership in the 2000s, but the heads of companies retained their autonomy and were involved in bureaucratic fights with Roscosmos. Then, Roscosmos merged with state-owned United Rocket and Space Corporation to create the Roscosmos state corporation. This new state corporation has been criticized as being like the old Soviet model with no incentive other than to follow instructions from political leaders. Other recent developments include Russian plans for a new space system including systems for intelligence and warning of air and space attacks and destruction and suppression of forces and means of air and space attacks. In 2015, the Russian Space Forces (established in 1992) was merged as a new branch of Russia's Aerospace Defense Forces responsible for monitoring space objects, identifying potential threats to the nation from space, and preventing "attacks as needed" (Jotham 2018). This branch combines elements of space forces, air forces, as well as air and missile command. Meanwhile, US President Trump has been considering whether and how to separate space activities from the Air Force evidenced in his executive order in June 2018 to create a new Space Force.

Russia has continued to work on ground facilities to control orbit and wage electronic warfare by targeting space communication and navigation systems. It allegedly jammed GPS signals during the Crimean conflict in 2014 (Harrison et al. 2018). Luzin wrote in 2016 that outer space communications and reconnaissance remain the Achilles' heel of the Russian Army (Luzin 2016). However, during the Syrian conflict, Russia used reconnaissance aircraft in addition to Soviet-era Vishnya-class intelligence-gathering vessels (AGIs) and ground-based SIGINT (Signals Intelligence) facilities on Syrian territory (Hendrickx 2017). Nevertheless, for now Russia remains dependent on airborne, sea-based, and ground-based reconnaissance assets to complement satellite data. The US Director of National Intelligence, Daniel Coats, concluded in 2018 that "Russia aims to improve intelligence collection, missile warning, and military communications systems to better support situational awareness and tactical weapons targeting... Russia plans to expand its imagery constellation and double or possibly triple the number of satellites by 2025" (Coats 2018).

Russia also allegedly has, or is developing, new ASAT capabilities including direct energy lasers, interceptor missiles, maneuverable satellites, robotics, and electronic warfare (Weeden 2015; Mizokami 2018). (These are designed to blind US intelligence and ballistic missile defense satellites.) Although many of these remain unverified or denied by the Russian government, US experts believe that the biggest threats from outer space are "non-kinetic threats such as jamming satellite-based capabilities such as GPS and communications" and that Russia has sent micro-

satellites into space which could be used to ram another satellite or snoop on it to collect data or interfere with its capabilities (Daniels 2017). Russia is also developing ballistic missile defense (BMD) capabilities, which are centered around Moscow with plans for a national missile defense dome. Missile defense capabilities may have dual function as ASATs, particularly systems deployed around the Kremlin. Russia has reportedly carried out the world's longest test of a surface-to-air missile system. Its efforts to develop hypersonic glide vehicles are argued to be explicitly aimed at evading US missile defense systems.

Addressing the Russian Military Academy of the General Staff in March 2018, Army General Valery Gerasimov announced that the next phase of Russia's new high-tech approach will focus on robotics, artificial intelligence, and the information and space spheres as well as on economic and nonmilitary targets (Tucker 2018). This approach is likely to continue. It is reactive to increases in the US military budget, as well as to rapid technological developments, and is part of a larger effort to move possible conflicts into areas of "nontraditional warfare." However, despite all its modernization programs, upgrades, and plans, Russia continues to be weak in many space systems, and many argue that long-term structural weaknesses affecting the broader economy, such as an aging work force, inefficiency, and brain drain, have still not been resolved. (Details about Russia's development of a long-term strategy since 2012 can be found on Anatoly Zak's website RussianSpaceWeb.com.)

## Russia's Space Diplomacy

Russia's strategy on outer space security issues since 2000 has also included diplomacy, just as it did in the Soviet period. Previously, the Soviet Union co-sponsored the Partial Test Ban of 1963 and the landmark Outer Space Treaty (OST) of 1967. Soviet delegates were active at the Conference on Disarmament (CoD) to promote discussion on the "Prevention of an Arms Race in Outer Space" (PAROS). (The CoD, a 65-member body in Geneva, is supposed to serve as a United Nations' forum for discussing multilateral agreements on arms control and disarmament. Since 1994, the CoD has been deadlocked due to competing priorities. CoD needs unanimous agreement to move forward on issues and set agenda. PAROS gained near-universal support in annual UN General Assembly resolutions, but the USA has consistently objected arguing that space weapons cannot be defined or effectively verified.) Under Putin, Russia has used the United Nations and its affiliated bodies to attempt to develop binding laws, non-binding norms, and transparency and confidence-building measures (TCBMs) to prevent and to control the use of weapons in space. Russia's official rhetoric is that it cooperates with states that share its goals and preference for inclusive negotiations at the UN. Certainly, Russia's diplomatic activism reflects a desire to participate in international organizations and fora to shape international rules, but it may also be a strategy to hedge its comparative economic and military weaknesses. Russia participates in the UN as part of a broader attempt to develop relations with other states of the emerging "multipolar international system" and as a platform to denounce what Russia

perceives as the US role in undermining the international rules of the game (e.g., the US unilateral pulling out of the ABM treaty but also Western military operations that lack the UN Security Council's mandate, Iraq and Kosovo).

Russia introduced a working paper in 2002 and then two more in 2004 at the CoD. These became the basis for the 2008 Russia-Chinese Draft Treaty on "Prevention of the Placement of Weapons in Outer Space and the Threat or Use of Force Against Outer Space Objects" (PPWT). This draft treaty extended the OST prohibitions on placement of weapons of mass destruction (WMD) to all forms of weapons. It sought to ban "any device placed in Outer Space, based on any physical principle, specially produced or converted to eliminate, damage or disrupt normal function of objects" (CD 2008). As Paul Meyer explains, "the termination of the ABM Treaty meant the elimination of the only prohibition on space-based weapons agreed upon beyond the ban on WMD in the 1967 Outer Space Treaty" (Meyer 2016). As mentioned above, Russia equates space weapons with weapons of mass destruction (WMD) and has consistently argued that their deployment would have a destabilizing effect on the global strategic balance. The US and other critics of the PPWT argued that the Russia-China treaty did not include a verification mechanism; it only limited deployment, not building of weapons, did not include terrestrial-based ASAT weapons, and did not resolve the problem of how to define a "weapon." (Although given the inherent ASAT capability of ballistic missile interceptors, any effort to include ground-based systems runs up against US commitment to deploy ballistic missile defense.) In response, in June 2014, Russia and China presented a revised version of the PPWT, which included a new article acknowledging the need for verification measures and suggested that these could be elaborated in a subsequent protocol to the treaty.

However, further consideration of the PPWT was prevented by the general blockage of the CoD, and Russia and China have not taken the draft to another forum. They prefer the CoD which protects their interests and gives them a voice and legitimacy. Unsurprisingly, Russia also opposed the 2008 EU Draft Code of Conduct for Outer Space (and its latest draft of March 2014) arguing that the EU code is undermining the work of the UN on space security. Russia and the BRICS argue that the proper format for such deliberations must be inclusive and consensus-based multilateral negotiations within the framework of the UN, in order to take into consideration all states' interests.

Since 2005 Russia has also solicited and proposed ideas for nonlegally binding and voluntary TCBMs (transparency and confidence-building measures) at the UN General Assembly. A UN Group of Governmental Experts (GGE), chaired by Victor Vassiliev, head of the Russian delegations to the UN GGE, produced a report in 2013 that enumerates several potential transparency and confidence-building measures, including information exchange, risk reduction measures, visits to space-related facilities, and consultative mechanisms (UN General Assembly 2013). This report led to subsequent UNGA resolutions encouraging states to review it. To quote Vassiliev (2015): "...we tried to put forward proposals that were practical, implementable, did not undermine sovereign rights or security of States." In 2018–2019, a new GGE examined possible legal instruments to prevent an arms

race in outer space, including the prevention of the placement of weapons in outer space. Since the CD remains in a state of paralysis, this means that Russia and China showed some creativity and found another platform for official work on their PPWT and other possible legal instruments. However, the GGE was unable to release its report because of last-minute opposition by the US representative.

As a final example of Russia's active diplomacy, Russia has also been pushing a "no first placement of weapons in outer space" resolution which was adopted by the UN General Assembly in 2015. This resolution, critiqued by the USA for not being truly transparent, encourages states to adopt a political commitment not to be the first to place weapons in outer space. In 2016, Russia and Venezuela (after years of Russian loans and weapon deals to Venezuela) released a joint statement to the CoD declaring that they will not be the first to deploy any type of weapon in outer space.

---

## Conclusion

For Russia, outer space has become an important area through which to respond to or negate Western strategy and capabilities as well as influence global norms. Its economic, military, and technological weaknesses relative to the USA and NATO have led it to pursue asymmetric tactics including working through bodies affiliated through the UN which give it publicity and some legitimacy but little ability to make real progress. Asymmetrical tactics adopted to advance their goals include traditional, new, and hybrid military capabilities, use of denial and uncertainty about Russian intentions, information, cyber diplomatic negotiation and cooperation, and legal means (including attempting to develop or reinforce norms) (Jackson 2019). The separation between global security and governance is not distinct. Russia's outer space strategy fits within its security and foreign policy efforts which focus on asserting Russia's authority, status, and prestige. Military efforts are but one part of a complex set of tools, which include not only outer space and new technology such as electronic warfare but also nonmilitary means (negotiation, finance, propaganda, etc.) employed to navigate what Russia perceives as an increasingly hostile world.

This situation is likely to become even more complicated. Outer space is increasingly interrelated with land, sea, and air and cyber domains. It also is increasingly congested with other state and non-state actors, including private companies. This proliferation of actors is taking place just as military strategies are increasingly forced to consider the "battlefield" as a seamless whole.

Today, tensions between Russia and the USA are high, and each recognizes what is sometimes called "an integrated multi-domain threat" coming from the other. This is reinforced by recent technological advances and significant distrust about each other's intentions. The result is the growing militarization of space. A pressing challenge for the future will be how to reconcile different security perceptions of states as well as non-state actors and their understandings about how the laws of armed conflict apply to military (and even civilian) space activities. For example, how does one define proportionality of response to an attack on a satellite? Is radio

jamming a use of force or an armed attack? Which activities are legitimate, and which are not? There is a plethora of ambiguity. The goal of creating the sustainable use of space for peaceful purposes and for the benefit of all humankind seems ever elusive.

---

## References

- Charron A, Fergusson J (2018) From NORAD to NOR [A] D: the future evolution of North American Defence Cooperation. Policy Paper, May, Canadian Global Affairs Institute, Toronto
- Coats D (2018) Worldwide threat assessment of the US intelligence community, congressional testimonies, 13 February. <https://www.dni.gov/index.php/newsroom/congressional-testimonies/item/1845-statement-for-the-record-worldwide-threat-assessment-of-the-us-intelligence-community>. Accessed 02 Apr 2018
- Conference on Disarmament (2008) Draft 'treaty on the prevention of the placement of weapons in outer space, the threat or use of force against outer space objects, February 29, 2008, CoD/1839
- Daniels J (2017) Space arms race as Russia, China emerge as 'rapidly growing threats' to US. CNBC, 29 March. <https://www.cnbc.com/2017/03/29/space-arms-race-as-russia-china-emerge-as-rapidly-growing-threats-to-us.html>. Accessed 2 Apr 2018
- Gareyev MA (2009) Issues of strategic deterrence in current conditions. *Military Thought* 18(2):1–5
- Harrison T, Johnson K, Roberts TG (2018) Space threat assessment. CSIS, Washington
- Hendrickx, Bart (2017) Russia encounters hurdles in satellite development and expansion. *Jane's IHS Markit*, 21 June
- Jackson N (2019) Deterrence, resilience and hybrid wars: the case of Canada and NATO. *J Mil Strateg Stud* 19(4):104–125
- Johnson-Freese J (2017) *space warfare in the 21st century: arming the heavens*. Routledge, Abingdon
- Jotham I (2018) Russia's 'Space Forces' just completed the construction of two new radar facilities, 1 February, *International Business Times*. <https://www.ibtimes.co.uk/russias-space-forces-just-completed-construction-two-new-radar-facilities-1657957>. Accessed on 2 Mar 2018
- Luzin P (2016) 'Russia's position in space. *Foreign Affairs*, September. <https://www.foreignaffairs.com/articles/2016-09-21/russias-position-space>. Accessed 2 Mar 2018
- McDermott, Roger (2012) Russia's 'New Look' military reaches out to space. *Eurasia Daily Monitor* 9(140)
- Meyer P (2016) Dark forces awaken: the prospects for cooperative space security. *Nonproliferation Rev* 23(2–3):495–503
- Mizokami K (2018) Russia, China will have anti-satellite weapons 'within a few years'. *Popular Mechanics*, 15 February. <https://www.popularmechanics.com/military/weapons/a18197465/russia-china-anti-satellite-weapons/>. Accessed 2 May 2018
- President of the Russian Federation (2011) The presidential decree 'On the approval of the priority directions of science and technologies of the Russian Federation' approved by the President of the Russian Federation on July 7, 2011, no. 899
- President of the Russian Federation (2015) The Russian Federation's National Security Strategy, 31 Dec 2015
- Roffey R (2013) Russian science and technology is still having problems -implications for defence research. *J Slav Mil Stud* 26(2):162–188
- Russian Government (2015) Russian assessment of the US global ABM defence programme – International security and disarmament, 5 Mar 2015
- Russian Security Council (2014) The military doctrine of the Russian Federation, 25 Dec 2014



- Tucker P (2018) Russian military chief lays out the Kremlin's high tech war plans, *Defense One*, 28 March. <https://www.defenseone.com/technology/2018/03/russian-military-chief-lays-out-kremlins-high-tech-war-plans/147051/>. Accessed 2 Apr 2018
- UN General Assembly (2013) Group of Governmental Experts on Transparency and Confidence building Measures in Outer Space Activities, A/68/189, Sixty-eighth session, July 29, 2013
- Vasiliev V (2015) Statement at the Joint Ad hoc meeting of the First and Fourth Committees of the 70th session of the UN General Assembly, 22 October 2015. [www.reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com15/statements/22October\\_SpaceGGE.pdf](http://www.reachingcriticalwill.org/images/documents/Disarmament-fora/1com/1com15/statements/22October_SpaceGGE.pdf). Accessed 2 May 2018
- Venet C (2015) Space security in Russia. In: Shrogl KU et al (eds) *Handbook of space security*. Springer, New York, pp 355–370
- Weeden B (2015) Dancing in the dark redux: recent Russian rendezvous and proximity operations in space. *The Space Review*, 5 October
- Zak A (2018) Russian space program in the 2010s: decadal review, 6 April. [http://www.russianspaceweb.com/russia\\_2010s.html](http://www.russianspaceweb.com/russia_2010s.html). Accessed 8 Apr



# Development of a Space Security Culture: Case of Western European Union

# 22

Alexandros Kolovos

## Contents

Introduction .....	401
The Western European Union Era (1955–2001) .....	403
The WEU and Space (1979–1999) .....	405
The Development of a WEU Space Security Program .....	406
Toward a WEU Space Policy .....	411
Conclusion .....	415
References .....	417

## Abstract

This paper deals with the origins of the European space security and defense effort. The main thrust of the argument in this paper runs as follows. All institutional space security and defense discussions were facilitated by an existing space security culture in Europe. This culture goes back several decades. The main institutional actor which paved the way for its creation was the Western European Union. The WEU now may have ceased to exist, but its space security culture it created remained. As such it facilitated the EU to recognize the importance of space activities in its Common Security and Defence Policy.

## Introduction

On 15 November 2002, the European Commission (EC) held an informal workshop in Brussels to examine the security aspects of space (European Commission 2002). The meeting was in the framework of a forthcoming Green Paper on the future of

A. Kolovos (✉)

Automatic Control, AirSpace Technology, Defence Systems and Operations Section, Hellenic Air Force Academy, Athens, Greece

e-mail: [alexandros.kolovos@hafa.haf.gr](mailto:alexandros.kolovos@hafa.haf.gr)

Europe in space, which would be the base to create a “White Paper” on the subject. This task had been given to the Commission by the Parliament, and among issues to be debated were political sensitive issues including space security and the needed institutional arrangements (The term *space security* is used according to the definition given in the introduction of the first volume of *The Handbook of Space Security (HbSS)* which states: “For the purpose of the HbSS, we understand space security as having two dimensions, security in space and security from space” (Schrogl et al. 2015). This chapter deals only with the second dimension that is security from space.). The Commission was concerned of the security aspects of space, and the reason of the meeting was to give contribution on the development of a Green Paper, which should highlight all the questions that should be answered in a White Paper.

Some of the main questions to be addressed at this workshop were “to define if Space is relevant for Security, how to merge civilian with security (dual-use), if Europe wants to be an actor in the space sector or prefers to buy the technology, or if EU wants to set up a cooperation with the US.” Nowadays the first question might raise an eyebrow in surprise. Although the Commission would be the owner of both the Green and White Papers, the reality was at the time that the EC had not been institutionally involved with the security issues before, due to the institutional limitations imposed by the Treaty on European Union.

Maastricht Treaty created an overarching structure to be known as the European Union (EU) comprising three components or *pillars*. The European Commission constituted the first pillar, while the Common Foreign and Security Policy (CFSP) was established as the second pillar. The third pillar dealt with aspects of the area of freedom, security, and justice. Until that time, the Commission has focused more on scientific programs and civilian space applications. Connections between space and security have not been central to most EU documents and were only partially addressed in its official space reports.

At the workshop it has been stressed that the Commission would have been glad if this task could be coordinated internally within the Council General Secretariat (CGS) of the second pillar so that the final outcome could be coherent. CGS could look in the space aspects within CFSP (Common Foreign and Security Policy) and ESDP (European Security and Defence Policy) concerning security.

This approach was chosen due to the fact that while these two policies had been established some years before (CFSP in 1992 and ESDP in 1998), their reflections had not appeared in any of the relevant space documents the Commission had produced. While initially this might considered as an absence of mechanism for policy coordination, actually it was more an institutional duty, due to the limitations of the first (EC) and second pillars (security and defense). Lisbon Treaty of 2009 would make the pillar structure obsolete.

The talk was of “security” but without defining the scope. At a working level, it was clear that the scope was environmental security, as it was evident by the development of the Global Monitoring for Environment and Security (GMES) program. This created a risk that it was perceived at higher levels as also covering those areas that fall within the second pillar. It was clear that the Commission was not on the same footing as the Council General Secretariat within the ESDP (European

Security and Defence Policy) and CFSP (Common Foreign and Security Policy) policies concerning space and security. EC thus acknowledged that no matter how much schooling, it was still difficult to think like the people of a particular culture if one is not working in that environment. The Commission as a responsible actor needed to take a well-prepared collective view.

It was due to this reason that the EC itself wanted some directly involved people to help them to find issues to bring in the security aspects of the Green Paper. Apart from its bodies, the Commission invited the EU Military Staff and representatives from three defense ministries (the UK, Belgium, Greece) that were active in space security (both nationally and in the Western European Union framework).

This specific task was finally implemented successfully, and the Green Paper addressed the sensitive topic of security dimension (European Commission 2003), because the Commission seemed to know exactly who were to ask. And this became possible due to an existing but almost unrecognizable cause, a preexisting space security culture. Cultures are about shared values. Space has always had its big players along the not so advanced players, but the glue in any community is that all of players have something in common even if their institutional circumstances vary.

This space security culture was created at the Western European Union framework, an organization that came into being with the ratification of the modified Brussels Treaty on 6 May 1955. Many people may not be familiar with this, since the relevant literature is rather limited. Key officers enabled in the Green Paper process, from the Council General Secretariat or as national experts, were previously enabled in WEU's space activities.

This chapter pays a long overdue tribute to the previously unknown by many contribution of the WEU in the development of this space security culture. Whereas all political and operational functions of WEU ceased and were transferred to the EU's European Security and Defence Policy in December 1999, its space security culture has been consolidated and preserved. Its influence at the EU was significant in the making of space security policy, as it helped creating, among others, two milestones: shaping the development of the 19 May 2003 General Affairs and External Relations Council (GAERC) decision which for the first time "recognised the importance of space applications and functions needed in order to enhance EU capabilities to carry out crisis management operations" (Council of the European Union 2003), along the Council's decision on "ESDP and Space Policy" (Council of the European Union 2004).

---

## **The Western European Union Era (1955–2001)**

Before we examine the space security activities of the WEU, it is considered useful in the analysis that will follow to give some basic facts regarding WEU. The Western European Union, as the successor to the Brussels Treaty Organization (founded in 1948), was a defensive alliance composed by seven founding members (Britain, France, West Germany, Italy, Belgium, the Netherlands, and Luxembourg). In its final synthesis (after 1995), WEU consisted of ten member states: the original seven

plus Portugal, Spain, and Greece. It was responsible to provide the framework for the creation of a European defense policy until 2001 (European External Action Service 2016). Located in Paris, WEU was created in postwar Europe as the responsible body for European defense and security issues, as these two domains were left outside the European unification attempt that had begun in the 1950s with the creation of the European community (Hatjiadoniu 2000).

In the mid-1980s WEU has been established as the forum to discuss European reactions in several challenges, like the response to a US invitation to Europe to participate in the US “Strategic Defense Initiative” or to the Euromissile crisis which created tensions in the US-European relations. As it was stated in 1986, “WEU has thus become established as the one European body in which space policy is discussed in all its aspects, military and civilian, taking into consideration the diverging viewpoints held by the various European countries” (Voûte 1986). It was a time when both the USA and USSR put heavy emphasis on military space programs, while Europe had no significant military space involvement. On the other hand, in January 1985, the Council at ministerial level of the European Space Agency (ESA) adopted an ambitious long-term European space program, with a purely civilian character.

The Maastricht Treaty, signed in December 1991 (and entered into force in June 1993) which had established the Common Foreign and Security Policy (CFSP), stipulated that it was the Western European Union which would elaborate and implement the development of a European security identity and more specifically the development of a “Common European Security and Defence Policy (CESDP) and a defence role within the European Union.” At the same time WEU acted as the European pillar of NATO with a task to enhance the role and responsibility of the European members within the alliance, namely, the “European Security and Defence Identity (ESDI) within the NATO.”

The Article J.4 of the Treaty on European Union (Maastricht, 7 February 1992) that followed stated:

1. The common foreign and security policy shall include all questions related to the security of the Union, including the eventual framing of a common defence policy, which might in time lead to a common defence.
2. The Union requests the Western European Union (WEU), which is an integral part of the development of the Union, to elaborate and implement decisions and actions of the Union which have defence implications.

The WEU declaration, adopted on that occasion, constituted the initial step in the development of the CESDP. In the declaration WEU member states agreed to strengthen the role of WEU as the defense component of the EU and as the means to strengthen the European pillar of NATO. That led to the initialization of a reflection at the WEU on the question of Europe’s future in the security and defense domain with a focus to examine and reinforce common means for action.

Based on the Maastricht provisions, WEU started to formulate and to develop its own crisis management procedures. In this period of time, the WEU entered its “operational” phase, adapting to the new post-Cold War conditions. Elements of

relatively successful adaptation include enlargement, missions, and especially its Petersberg tasks. At the Petersberg ministerial meeting in 1992, WEU member states defined the crisis prevention and management missions that could be conducted through WEU by their forces as follows: “military units of WEU member states acting under the authority of WEU could be employed for: humanitarian and rescue tasks; peacekeeping tasks; tasks of combat forces in crisis management, including peacemaking.”

In 1997, the Treaty of Amsterdam amended the Treaty on European Union (Maastricht 1992). The relationship between the EU and WEU is contained in the second paragraph of Article 17(1). This states that “The Union shall foster closer institutional arrangements with the WEU with a view to the possibility of the integration of the WEU into the Union, should the European Council so decide. It shall in that case recommend to the member states the adoption of such a decision in accordance with their respective constitutional requirements.”

Finally the European Council decided to give the EU the capacity for independent action, backed up by credible military forces. In December 1999, WEU surrendered political and operational work to the EU (and its European Security and Defence Policy – now known as Common Security and Defence Policy (CSDP)) (Bailes and Messervy-Whiting 2011). In 2001 all functions of the WEU have effectively been incorporated into the EU. With the introduction of the Lisbon Treaty (2009), the EU’s role was greatly increased, so the European Parliament to avoid duplication called for the abolition of the European Security and Defence Assembly (ESDA)/ Assembly of WEU (The Assembly of WEU was founded in 1954 by the modified Brussels Treaty. Composed of 364 national parliamentarians from 28 countries including all EU member states, the Assembly scrutinized European intergovernmental activities in all areas of security and defense. ESDA was debating space- and security-related topics. Following the transfer of WEU’s operational activities to the EU, the Assembly also acted as the interim European Security and Defence Assembly.). It was agreed subsequently that WEU would be wound down completely by May 2011 (Remuss 2015).

---

## The WEU and Space (1979–1999)

WEU’s interest in space activities goes back to its first parliamentary Assembly report on “Space War or Space Cooperation?” in 1961 (Assembly of Western European Union 1961). A new report on “European Space Organisation” came in May 1962. Then in the mid-1960s, WEU studied the possibilities of setting up a European satellite agency for the verification of arms control agreements, for monitoring crisis situations, and, last but not the least, for intelligence gathering (Assembly of Western European Union 1988a; Heintze et al. 1993).

The WEU Assembly and especially its Technological and Aerospace Committee continued to advise on the evolution of European military and civilian space activities in the framework of European security all through the 1980s (Assembly of Western European Union 1984). A relevant role to a smaller degree to promote

public awareness had the WEU's Institute for Security Studies. In 1985 the Technological and Aerospace Committee convened a colloquy regarding the space challenge for Europe (Assembly of Western European Union 1985). The time was right as the ministers of foreign affairs of the then seven countries tried to coordinate their answers to the US President Reagan's proposal to the European members of the Atlantic Alliance to participate in the Strategic Defense Initiative (SDI) which he just had announced.

The seeds of development of the European cooperation in space activities for security purposes have been on WEU's agenda since 1979 (Assembly of Western European Union 1990). The cooperation effort focusing on an earth observation satellite system program started officially on 13 November 1989, when the WEU Ministerial Council Decision in Brussels set up an ad hoc subgroup on space (SGS), the so-called Space Group. Its mandate was to study the possible uses of space technology in three specific areas: the verification of arms control, the monitoring of crises affecting European security, and the monitoring of environmental hazards (Assembly of Western European Union 1988b, McLean 1995). The WEU's Military Staff participated in the Space Group since its inception (The Military Staff was responsible for the implementation of policies and decisions as directed by the Council and Military Committee. It prepared generic and contingency plans, carried out studies, and recommended policy on matters of an operational nature under WEU politico-military control.).

## **The Development of a WEU Space Security Program**

While some major European space-faring nations which were members of the WEU had access to military space systems from the 1970s, the turning point of the institutional European approach in the security and defense domain is found, in our judgment, in two significant incidents: the Chernobyl nuclear reactor accident and the first Persian Gulf War.

On 26 April 1986, a nuclear accident happened at the Chernobyl plant in near Pripjat, Ukraine, in the then USSR. On 29 April 1986, the US Landsat 5 was the first civilian satellite to reveal the burning reactor n°4 caused by the explosion. But its imagery resolution was comparatively poor, being on the order of 30 m. Then 2 days later, on 1 May 1986, just 2 months after its launch, France's SPOT 1 acquired the first 10-m high-resolution imagery, which showed a plume of hot air trailing from the reactor building. Initially the Soviets decided to downplay the catastrophic nature of the event, and only on 14 May 1986, General Secretary Gorbachev spoke about the disaster. At that time the scientific community had realized that the pollution was expanding throughout Europe despite the political messages stating that the pollution will stop at the Ukrainian border. Satellite imagery of Chernobyl marked also the first time the mass media used space surveillance which showed that large-scale activities cannot be hidden or protected by borders. These conclusions were included in two Assembly reports and were sent

to the WEU Council. The latter, politely thanked the Assembly for the job done. No action was taken.

But the decisive point for Europeans was the first Persian Gulf war after Iraq occupied Kuwait on 2 August 1990. Coalition Forces, led by the USA, with the cooperation of France and UK forces, began a military deployment which led to the 17 January 1991 active air campaign against Iraq. The Persian Gulf War (1990–1991) international conflict revealed significant lessons to be learnt not only from the British and French personnel involved in the coalition against Iraq but for the Europeans as a whole.

Called also as “the first space war,” it highlighted publicly that information from space was a valuable political and military tool for the execution of operations (including Petersberg). It was also an alarm of the weakness shown. On behalf of the Europeans, it was WEU who begun to respond practically by further exploiting the military aspects of space. WEU was first to recognize the relationship between military space activities and their common security. The common political will, shown on the decision for the creation of the WEU Satellite Center 1992, proves that it was also the first time all WEU countries have worked together identifying space as a common mean of action in the security and defense domain.

One outcome of the Gulf War was the wide acceptance of the vital role that satellites played (Kiernan 1991; Gupta 1991). It was in this framework that the European forces felt that their assets and capabilities would not enable them to participate fully and on an equal basis as desired with the Americans. As French Minister of Defense Pierre Joxe put it: “In the Persian Gulf War, without the American intelligence, the european Allies were almost blind. It was the United States who provided, whenever they want it, the necessary intelligence to carry out the war” (De Selding 1991a). Furthermore, the contributing European forces realised the overall US dependence on space.

The Gulf War was the main relevant event where the European Defence Ministers understood how much the EU was dependent to the USA for the global evaluation of a situation and how much space was the solution. After the Gulf War, WEU was convinced that space-based observation represented a strategic capability which was needed to acquire, in order to meet its security and defense responsibilities (Assembly of Western European Union 1991). As such a multipronged approach has been followed:

### **At the Ministerial Level (Foreign and Defense Ministers)**

1. The establishment of the Satellite Center (WEUSC). In April 1991, in Vianden (Luxembourg), WEU Ministerial Council decided the creation of a Satellite Center (SatCen) to be later based at Torrejon Air Base (near Madrid, Spain). The creation of the Satellite Center was for a trial period of 3 years, from 1993 to 1995. The cost of this venture was high (38 million ECU for the first 3-year experimental phase) (Molard 1998). According to its Concept Paper (WEU Council of Ministers 1997), the main function of the Satellite Center (which was officially inaugurated in 1993) was to analyze for security purposes imagery



from satellite and airborne sources relating to areas of interest to WEU and to train European experts (WEU General Secretariat 2000). SatCen depended largely on commercial imagery and on national provision of imagery. SatCen's establishment was a rare political move which gained the consensus of all member states at the time. It was also a unique model in itself in relation with the sharing of satellite-generated information at the EU level. It was the first occasion in WEU which a part of a space program (i.e., the creation of a photointerpretation operational center) preceded the policy meant to implement. At the Ministerial Council in Lisbon (1995), the WEU Satellite Center was declared a WEU permanent subsidiary body and was placed under the authority of the WEU Council. Citizens of the ten full member nations were its staff, while image analysts from member states and associate members could be second personnel for a limited time. Furthermore, SatCen educated national experts via its training activities which also comprised participation in seminars, conferences, and "field" visits.

2. *Toward an independent European space-based observation system for defense.* The Ministerial Council held in Bonn on 18 November 1991 decided to study the feasibility of an independent European space-based observation system for defense purposes in 1992–1993 period. That decision reflected WEU's willingness and determination to move ahead. The President of the Assembly, which had only consultative powers, welcomed these decisions which responded to recommendations the Assembly had been making for several years (Space Policy 1991). Two types of studies were conducted:
  - System concept-related studies consisting of the Main System Feasibility Study at a cost of 4.5 MECU, led by DASA/Dornier company (Assembly of Western European Union 1992), along with seven special studies addressing additional critical aspects of the satellite system (simulation, fusion, sensors) at a cost of 0.7 MECU.
  - Benefit assessment studies aimed at assessing the operational suitability of the most promising satellite system solutions at a cost of 1 MECU. These preliminary studies provided a general overview of what could be offered by a WEU Earth Observation System.

In Kirchberg Declaration on 9 May 1994, "Ministers confirmed the aim of further developing WEU's capability to use satellite imagery for security purposes [...] reaffirmed their will to set up an independent European satellite system. A decision would be taken subject to evaluation of the costs and merits of the proposed system and of other WEU alternatives and affordability."

The final outcome from these studies was that a satellite system fully compliant with the Main System Feasibility Study has been shown to be complex and costly. WEU member states envisaged an interim solution to be proposed after discussions with the user community aimed at refining the requirements. As a trade-off, a new (phase A) study has been proposed, and its estimated cost was in the order of 30 MECU.

### At the Space Group Level

1. *Participation in a developing multinational program.* Also WEU's Space Group decided to explore further engagement in activities toward a possible WEU participation in a developing multilateral program (the then Helios-1 program). Helios was the only successful example of a multilateral collaborative military space effort in Europe. French Defense Minister Joxe had repeatedly stated that all WEU member states could participate in the Helios-1 program that was underdevelopment. Of the seven WEU members, Italy and Spain choose to participate.
2. *Procurement of imagery from commercial systems.* The Space Group tasked the SatCen to explore further on other solutions which might overcome limitations on the timeliness of the WEUSC response to tasking. Finally, of several possible options, that chosen was the transmission of images via high data-rate links.

In Lisbon on 5 May 1995, Ministers of Foreign Affairs and Defence of the WEU nations tasked the Space Group “to continue its activities, concentrating on the last three proposed approaches to develop a WEU capability to use satellite imagery for security purposes, namely: The establishment of a WEU earth observation (EO) satellite system, the participation in a developing multinational programme and the procurement of imagery from commercial systems.”

Ambassador Horst Holthoff, WEU's Deputy Secretary-General, addressed the main reasons for all these decisions in 1995. An autonomous observation capability to provide appropriate intelligence is a prerequisite for a functioning European policy on security and defense. The EO satellite system is a way for Europe to become an equal partner with the USA in exchanging satellite imagery which might lead to technological cooperation. Also this EO system would support the European aerospace industry, which had experience in participating in European programs and keep it ready for international competition. And finally it can become a tool for accelerating European integration (Holthoff 1995).

### WEU's Ambition: An Independent EO System for Defense

For the Earth Observation domain, as a first target, WEU sets the goal of an independent European space-based observation system for defense, enabling the WEU to mount an autonomous operation without recourse to NATO command assets and capabilities placed anywhere on the spectrum of Petersberg missions.

That was very obvious from the following event. In March 1995 WEU organized a colloquy on Gran Canaria, regarding a European space-based observation system (Western European Union 1995). In this framework Gil Klinger, then US Acting Deputy under Secretary of Defense (Space), made a point of stressing that the US Department of Defense was keen to increase the level of cooperation between the USA and WEU with regard to space and space systems (McLean 1995). There was not a European consensus to follow this transatlantic cooperation road.

But the road to strategic independence faced obstacles since it could not gather the consensus of all member states. Some governments were hesitant by the order

of magnitude of the investment required for the development of an autonomous European Earth Observation System consisting of both optical and RADAR satellites. Since it was evident that there was not a consensus to move ahead, the WEU decided to follow more conservative solutions.

So in Madrid Declaration, the ministers, having in mind the high cost of the establishment of an independent program and knowing of the plans for the Helios-2 program, tasked the Space Group “to continue its activities by defining the basic conditions for possible WEU participation in a developing multilateral European programme, while in the meantime continuing with the procurement of commercial imagery and studying the possible WEU ground segment.” Thus, the following actions followed:

1. Regarding the participation in a developing multilateral European program, according to an Assembly report: “WEU’s participation in the Helios-2 programme is therefore not only desirable and necessary – it must also be feasible. [...]WEU should not expect to receive an offer from the Helios-2 participating countries but should express its desire to take part in the programme” (Lenzer 1996).
2. The WEU consultations to reach an agreement with the Helios nations (France, Italy, and Spain) on an improved access by the WEU to Helios-1 have been examined since 1992, after France reversed its position that Helios-1 imagery would be available only to its owners (De Selding 1991b). In 1993 the three Helios nations signed a Memorandum of Understanding for the WEU to get access to Helios-1 governmental imagery. It is important to notice that the MoU has been signed the day before the official inauguration of the WEU SatCen and also that this agreement was signed 3 years before the launch of the first Helios satellite. Access was given through a special Helios-1 cell which had been created at SatCen with limited access, due to the classification of Helios imagery at *SECRET* level, which was very complex and difficult to handle. This access to Helios-1 trilateral military photoreconnaissance program gave SatCen a truly European dimension.
3. Also, in 1996 the Space Group tasked SatCen to perform a feasibility study on medium- to long-term opportunities for operational satellite data reception at the WEU, including commercial imagery such as the ones provided by SPOT Image, RADARSAT, etc. (WEU Satellite Centre 1997).
4. Then at the 1999 WEU Luxemburg ministerial meeting, the WEU ministers gave SatCen a mandate to establish, before the end of year 2000, a midterm concept for improving access to satellite imagery (WEU Satellite Centre 2000). A study was launched on the options for setting up a European satellite observation system in the medium and long term.

Ministers in Bremen in May 1999 tasked the Space Group to continue its work on evaluating the possibilities for WEU participation in developing a multilateral European program and on studying questions related to a possible WEU ground segment, taking into account existing ground segments in WEU nations. In so doing,

close contacts were maintained between WEU SatCen and the relevant EU authorities, competent in the field of earth observation research and policies.

In November 2000, the relevant study was finalized, and SatCen was expecting a mandate from the WEU Council to initiate in 2001 the procurement process for a suitable receiving, processing, and archiving facility. But since in 2001, all functions of the WEU would have effectively been incorporated into the EU; no immediate decisions could be taken on the issue. Due to the demise of the WEU, these steps in space security program development, originally envisaged for 2001, would not take place under its auspices. The WEU's Satellite Center, along the Institute for Security Studies, had been transferred to the community framework. Also, since the Helios MoU was signed with WEU member states, this MoU was stopped as soon as the WEU SatCen has been transferred to the EU, which had a different list of member states.

## **Toward a WEU Space Policy**

While WEU's space activities were under development, at the institutional level, something was missing. All these actions constituted specific steps toward a WEU space program in the Earth Observation domain. Some steps had been already implemented, while others were at the study level. But, the WEU had not developed firstly an overarching space policy, under which this WEU space program was conducted.

This seemed odd since the Assembly of the WEU started to debate upon the space policy back in 1966, with its "Juridical problems and space policy report" (Assembly of Western European Union 1966). Ten years later, the issue resurfaced in a more general way. In 1976 WEU's Assembly Committee on Scientific, Technological and Aerospace Questions held the first colloquy in Toulouse to study what a European aeronautical policy might be.

## **Proposal for a WEU's Earth Observation Space Policy**

It was in this framework that on January 1998, the WEU Hellenic Presidency presented its program in which there was a conceptual idea for the formulation of a WEU's Earth Observation Space Policy (The Presidency of the WEU was held by member states in rotation for periods of 6 months. The Presidency influences the priorities for work in the WEU and sets the pace of meetings and their agendas.). The third point of Presidency's Program stated the following:

In an effort to further develop and enrich the exchange of views among nations on space related questions, Presidency wishes to launch a general discussion on elements that could constitute the framework of a WEU space observation policy. By initiating this exercise, we hope that this group could reach a common understanding on the fundamental guidelines, as well as the medium and long-term goals of a coherent WEU space observation policy.

Before presenting the idea, the Presidency made informal consultations with Germany (the former Presidency) and France, as the dominating power in space

issues in Europe (in the framework of the discussions investigating the possibility of Greece's accession to the forthcoming Helios-2 program). Both countries expressed their support. France argued that for a better presentation of the issue, it was necessary to draw up a relevant text to be put on the basis of discussion. For the drafting of the relevant text, the French side proposed further cooperation with the relevant WEU Technological and Aerospace Committee, which resulted in very positive comments.

Similarly, it agreed with the Greek option to include telecommunications and navigation issues in it, including examples of existing European cooperation in these two areas (the tripartite military Trimilcom satellite communications between the UK, France, and Germany (later to be failed), as well as the European EGNOS (European Geostationary Navigation Overlay System, under development at the time). But the opinion of the Hellenic authorities was that initiative should focus only in the Earth Observation domain, which was after all the nucleus of the WEU's space activities so far and the mandate of the WEUSC, in order to overcome any objections from other countries if the term "WEU space policy" was raised.

Formulating this document, apart from the relevant body of work from the WEU, and the advice from the Satellite Center and the Secretary of Aerospace and Technological Committee of the WEU General Assembly, the texts of space policies of other countries (France, the UK, Germany, the USA), along with informal consultations from the UK and Belgian delegations, have been taken into account. It was in this framework that on 27 February 1998, the WEU Presidency presented a first working paper entitled "WEU's Earth Observation Space Policy," which proposed a balanced conceptual framework to establish the formulation of such a policy (Hellenic Presidency 1998). This document is presented below for historical and research purposes.

"WEU's Earth Observation Space Policy" [SGS(98), Bruxelles, 27/2/1998]

**Introduction** For several years (since the Vianden decisions in June 1991), WEU has been engaged in continuing efforts toward a European earth observation space program. The first stage of this program was the establishment of a satellite image interpretation center (which constitutes the ground segment of WEU's space program). A second stage was the study on the possibilities for medium- and long-term cooperation on a European space-based observation system (the space segment). However WEU hasn't yet defined an Earth Observation Space Policy, under which its earth observation space program can be conducted. To this effect, the Greek WEU Presidency undertook the initiative to present a first working paper to the Space Group.

**Scope** This document provides the first draft for a framework to establish the formulation of WEU's Earth Observation Space Policy (EOSP). The principles and guidelines, with respect to the conduct of WEU's space program and related activities, could provide the basis for further discussions among delegations aiming at the development of EOSP.

**Main Objectives** The proposed goals of WEU's earth observation space activities are:

- To strengthen its operational role. The possession of up-to-date data is a key element for taking political decisions, and space observation systems can play a key role in this.
- To enhance the scientific, technological, and industrial potential of the WEU participating nations.
- To promote international cooperative activities, taking into account WEU's priorities and interests.

**Basic Principles** WEU earth observation space activities will be conducted in accordance with the following principles:

- WEU will make use of earth observation space assets for activities in pursuit of its security concerns and its operational needs.
- WEU shall support such activities as surveillance, reconnaissance, and environmental monitoring (including research and development of programs supporting these functions).
- WEU may use both commercial and noncommercial earth observation space systems to meet specific mission requirements.
- WEU should envisage the most effective use of existing earth observation European satellite and/or its participation in the development of an independent system. Such a decision should be based on an in-depth evaluation of the implied costs and benefits.
- WEU should also be ready to use and exploit other existing or emerging commercial space technologies and systems.
- WEU will ensure that its earth observation space program shall be conducted in accordance with its broader mission and policy and the deriving operational requirements.

**Policy Guidelines** The following ideas provide a framework through which the proposed policy in this document will be carried out.

- To fulfill its missions effectively, the Satellite Center will continue to strengthen its functional links with the Planning Cell and Situation Center.
- The Satellite Center should spare no effort to enhance its operational and technical capabilities, in order to further improve its effectiveness in undertaking the required tasks.
- WEU should continue the further training of its Satellite Center's staff in the development of digital image processing, photointerpretation and gathering, and exploiting accessible data.
- The Satellite Center will pursue the identification and development of appropriate applications deriving from its activities. Such applications will create new capabilities or improve the quality and efficiency of ongoing activities.

- WEU should also follow the developments in the field of European space transportation.
- WEU will encourage multilateral cooperation within its framework for the development, construction, and operational use of space observation systems.
- WEU shall encourage the further development of international cooperation, particularly when this has beneficial effects for European security interests and for European space industry. In this context, WEU should establish relations with the European Space Agency in order to determine possibilities for cooperation in space-based observation. It is hoped that this will develop a synergy between scientific and applications orientated programs.

### **Drafting a WEU's Space Policy**

Of a very general nature in order to gain all member states acceptance, this document has been discussed at various Space Group meetings and revised accordingly to the comments received by three WEU's permanent member states (France, the UK, and Germany). The WEU Military Staff and the WEU SatCen worked closely together in drafting the final paper.

Additionally it has been expanded too. To the original Presidency's initial chapters, three more were added:

- The first (Chap. *V Operational Requirements*) concerned the operational requirements that the WEU had to be fulfilled by satellite systems. They were submitted by the WEU Military Staff, following a remark during the reflections by the Greek Presidency that the operational requirements asked in 1996 by the Ostend Declaration were still pending. The latter in paragraph 30 stated that "the Ministers took note that the further in-depth study could only be continued after having defined WEU's operational requirements." Given this mandate and the time that has passed from 1995 which show the emergence of new technologies, the Presidency believed that the old requirements served its purpose at that time, but it was felt that further work to refine and expand its scope would be necessary, in order to evaluate the various options. WEU Military Staff addressed the issue.
- The next two chapters (*VI Role and Function of the WEU Satellite Centre* and *VII Improvements of The Satellite Centre's Operational Capabilities*) were submitted by Germany in the framework of balancing the relevant space policy text with the Concept Paper, which guided the WEUSC's work internally. Although the approval of the latter has been preceded in time, thematically, it was rather a subset of the text of space policy.

Finally, the Space Group, realizing the good spirit of the reflections between the member states, seized the opportunity to further reflect the importance of space and decided to expand the scope of the initiative, thus covering all aspects of space assets. The new domains of interest that have been added were the developments in navigation and positioning and communications.

The next Italian Presidency finalized the work, the Permanent Council approved the document on the “WEU Space Policy” and finally the ministers on November 1998 in Rome Declaration took note of this policy: “Ministers appreciated the finalization of work on a conceptual framework paper concerning WEU’s Space Policy, initiated by the Greek Presidency, and they took note of the relevant document, defining this policy” (WEU Council of Ministers 1998).

This final document has been released at the WEU members with a classification “RESTRICTED.” Due to the demise of the WEU, the further implementation of the *WEU Space Policy* could not take place.

---

## Conclusion

In this chapter we argue that the space security culture, which has been emerged in WEU, was consolidated, preserved, and continued serving well the EU, when the latter found itself institutionally responsible for the first time in its history to exercise fully its ESDP policy at the dawn of the new millennium. “The Wise Men” Report stated this: “European Security and Defence Policy is incomplete without a space component. ESDP relies on a mixture of civil and military instruments for crisis and conflict management” (Bildt et al. 2000).

The purely civilian EU space program, developing so far (such as GMES program), was just not enough to cover ESDP needs. The Commission admitted this in its 2000 “Europe and Space: Turning to a new chapter” report, which stated that “Dual-use (civilian-military) aspects of satellite systems have not so far figured highly on Europe’s agenda. Through the Satellite Center of the Western European Union (WEU), Europe has gained some experience in dual-use. Integration of the WEU Satellite Center in the EU may open new avenues for shared utilisation” (European Commission 2000).

WEU was there to provide its powerful vision regarding the use of space in the security and defense domain. The realization of the significant role that space plays in European common security resulted in an ongoing strong presence of WEU in the space in the ESDP domain. Even if one can characterize its approach as a little “unorthodox,” as it put the space program before its overarching space policy which followed, it was effective.

WEU around 2000 had conquered all the basic steps of the policy cycle in the space domain. These steps in public policy theory usually include agenda setting, policy formulation, policy implementation, and policy evaluation and change. WEU has set the agenda and has formulated its relevant policy, it has taken the decisions, and it has launched a space program which implemented this policy.

Furthermore it created a strong governance for space issues. With the help of an impressive body of work coming from the Assembly of Western European Union, a specialized governing body (the Space Group), along with the excellent leadership and staff gathered at the SatCen and with the cooperation of the European defense industrial technology base, WEU has paved the way for the first robust institutional



space program in Europe in the Earth Observation domain for its ESDP (For example, the EUROSPACE Security & Defence working group published quite a few reports demonstrating the capacity and willingness of the European industry to build the space architecture that the EU would need after having worked on its space policy. An evaluation of the cost of such a space system has even been announced: only 5€ per European citizen per year to be invested in a space system for European security. (Personal communication with General Bernard Molard, former Director of WEU SatCen and ASD EUROSPACE Security & Defence WG Chairman (March 3, 2019).).

Evaluating its pioneering studies that has focused on producing specialized and/or expensive satellite systems, WEU exercised a balanced approach in choosing cost-effective solutions when there was not a common political will. WEU and its bodies had the experience to undertake all of the tasks listed above, but not the resources to do them all. Furthermore the economics at that time limited the willingness of MS to contribute more resources. WEU showed a specific restrained culture to not pay any price to achieve the stated goals but chose to expand its capabilities in a very cost-effective approach.

WEU also created a “learning-centered work culture,” in which it was safe for members of its bodies to raise doubts. The case of prioritizing first the development of its space program and then its space policy and the issue of moving on with studies without having first defined specific operational requirements are examples of this learning culture of accepting and amending mistakes.

As the WEU has been absorbed by the EU, structures like the Military Staff still remained in the new scheme, along with some of the former WEU staff who participated in them or in other newly created bodies. The Commission wisely sought to benefit from them and from the lessons learned at WEU and considered how the most useful parts of this space security culture, which has been formatted in WEU, might be preserved. It is a task that in this new environment both the EU SatCen and the EU ISS aimed to further contribute (In its website, the EUISS states its aim to foster a common security culture. [https://europa.eu/european-union/about-eu/agencies/iss\\_en](https://europa.eu/european-union/about-eu/agencies/iss_en)). And the EU was eager to build upon it, at least at this early stage.

The following paradigm is self-explanatory. A 2002 report from WEU’s Technological and Aerospace Committee stated that “space applications can provide political decision-makers and in the EU with part of the information they need to carry out an effective European Security and Defence Policy (ESDP). Until now, the absence of political will has prevented the EU from adopting a proper space policy” (Assembly of Western European Union 2002).

Space is a “trans-pillar issue”; one has to deal with it from an overarching architecture. Only 2 months after the EU Hellenic Presidency of 2003 presented its initiative “ESDP and Space” (Kolovos 2009), the Military Staff, tasked by the WEU Military Committee to elaborate upon this issue, prepared an information paper entitled “Space Systems Needs for Military Operations” describing the areas in which space systems could improve EU military capabilities (European Union Military Staff 2003).

This was the first official document produced by a Council body on the ESDP requirements for space assets. The Military Staff was a new structure at the EU, but its space security culture was inherited from the old Military Staff. Then, on 22 November 2004, the Council approved the document “European Space Policy: ESDP and Space,” which provides the identified and agreed upon ESDP requirements to be reflected in the global EU space policy and its corresponding European space program.

In 2015, Frank Asbeck, former Director of the WEU SatCen and Principal Adviser for Space and Security Policy at the European External Action Service, stated that “Space has now been clearly recognized as a key element in the EU’s security and defence-related activities” (Asbeck 2015).

Verifying this statement in June 2016, the Global Strategy for the European Union’s Foreign and Security Policy addresses the issue of space as such, “First, European security hinges on better and shared assessments of internal and external threats and challenges. [. . .]. This requires investing in Intelligence, Surveillance and Reconnaissance, including [. . .], satellite communications, and autonomous access to space and permanent earth observation” (EU Global Strategy 2016). Almost 20 years ago, it was the WEU which had decided first to develop an independent European space-based observation system since it understood well this dimension.

Much of this recognition should be credited to the work done by WEU due to its space security culture. The WEU developed its space activities under the assumption that the civilian and military needs for all actions for ESDP purposes are compatible, with potential for synergies. WEU’s SatCen is still the only relevant CFSP/ESDP operational tool in the geospatial intelligence. SatCen exploited long before any other structure a “dual-use” approach, which was unique institutionally and paved the way for others to follow. WEU may be gone, but its space security culture established capabilities, and personalities were there to lead the EU in its early steps of recognizing space’s role in CSDP, and as such it is not forgotten.

---

## References

- Asbeck F (2015) Foreword. In: Schrogl K-U et al (eds) Handbook of space security: policies, applications and programs. Springer, New York
- Assembly of Western European Union. Proceedings Vol. III, seventh session, second part, Document 215, December 1961
- Assembly of Western European Union. Proceedings Vol. III, twelfth session, second part, December 1966, Document 388, Item no: WEU-22.011, 21/11/1966
- Assembly of Western European Union. The Military Use of Space, Report, submitted on behalf of the Committee on Scientific, Technological and Aerospace, Thirtieth Ordinary Session (First Part), Document 976, 15 May 1984
- Assembly of Western European Union. The Space Challenge for Europe: colloquy, Munich, Official record. Office of the Clerk of the Assembly of WEU, Paris 18th–20th September 1985
- Assembly of Western European Union. Verification: a future European satellite agency: report by Mr Fourré rapporteur, Proceedings Vol. III, Thirty-fourth session, second part, December 1988a, Assembly document 1159

- Assembly of Western European Union. Scientific and technical aspects of arms control verification by satellite, report by Mr Malfatti, rapporteur Proceedings, Vol. III, Thirty-fourth session, second part, December 1988b, Assembly document 1160
- Assembly of Western European Union. Observation Satellites, a European Means of Verifying Disarmament, Symposium, Technological and Aerospace Committee. Rome, Official Record. Office of the Clerk of the Assembly of WEU, Paris, 27th–28th March 1990
- Assembly of Western European Union. Weaponry after the Gulf War–New equipment requirements for restructured armed forces, 37 Ordinary Session, Document 1272, 14 May 1991
- Assembly of Western European Union. The development of a European space-based observation system, 38 Ordinary Session, Document 1304, 30th April 1992
- Assembly of Western European Union. A European Space-based Observation System, Colloquy, Official Record. Office of the Clerk of the Assembly of WEU, Paris, San Agustin, Gran Canaria, 24th–25th March 1995
- Assembly of Western European Union. European space observation vital for EU security, WEU Press Release, 5 June 2002
- Bailes A, Messervy-Whiting G. The demise of the Western European Union: lessons for European Defence, International Security Programme Rapporteur Report, 10 May 2011. [https://www.chathamhouse.org/sites/default/files/100511\\_bailes\\_0.pdf](https://www.chathamhouse.org/sites/default/files/100511_bailes_0.pdf)
- Bildt C, Peyrelevade J, Späth L (2000) Towards a space agency for the European Union. Report for the Director-General of the European Space Agency. Available from [http://esamultimedia.esa.int/docs/annex2\\_wisemen.pdf](http://esamultimedia.esa.int/docs/annex2_wisemen.pdf)
- Council of the European Union. Draft GAERC conclusions on ESDP (public), 9174/03, Brussels, 13 May 2003. <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%209174%202003%20INIT>
- Council of the European Union. European space policy: “ESDP and space”, 11616/04, 16 Nov. 2004. <http://register.consilium.europa.eu/pdf/en/04/st11/st11616-re03.en04.pdf>, par.1
- De Selding P. Calls for French Lead in European Spy satellite drive, Space News, May 13–19, 1991a, p 20
- De Selding P. Joxe: France to Share Helios Images with WEU, Space News, June 10–16, 1991b, p 22
- EU Global Strategy (2016) Shared vision, common action: a stronger Europe. A global strategy for the European Union’s foreign and security policy. High Representative of the Union for Foreign Affairs and Security Policy, Vice-President of the European Commission. <https://europa.eu/globalstrategy/en/global-strategy-foreign-and-security-policy-european-union>
- European Commission. Europe and space: turning to a new chapter. Communication from the Commission to the Council and the European Parliament – COM/2000/0597 final
- European Commission. Green Paper on the future of Europe in Space, Workshop on Security Aspects Brussels 15th November 2002, Research Directorate-General, Space Policy and Coordination of Research, Brussels, 26/11/2002, D(2002) CB
- European Commission. Green paper on European space policy: report on the consultation process – information document to the Joint Task Force 4 September 2003, Sec (2003) 1249 Brussels, 11.11.2003, <http://register.consilium.europa.eu/doc/srv?l=EN&f=ST%2014886%202003%20ADD%201>. European Commission, European security discussed at Athens, Green Paper consultation, 15 May 2003, [https://www.web.archive.org/web/20080205161946/http://www.ec.europa.eu:80/enterprise/space/news/article\\_598\\_en.html](https://www.web.archive.org/web/20080205161946/http://www.ec.europa.eu:80/enterprise/space/news/article_598_en.html)
- European External Action Service. Shaping of a common security and defence policy, 08/07/2016. [https://eeas.europa.eu/headquarters/headquarters-homepage/5388/shaping-common-security-and-defence-policy\\_en](https://eeas.europa.eu/headquarters/headquarters-homepage/5388/shaping-common-security-and-defence-policy_en)
- European Union Military Staff. Space systems needs for military operations, 9793/03, 27 May 2003
- Gupta V. METEOSAT lifted fog of war to expose reality in Gulf, DEFENCE NEWS, March 18, 1991
- Hatjiadoniu A. (2000) The Daedalus European security: the interactions of NATO, EU, WEU. NATO research fellowships programme 1998–2000. <https://www.nato.int/acad/fellow/98-00/hatjiadoniu.pdf>

- Heintze H-J, Wallner J, Hounam D, Nowak M (1993) Remote sensing and strengthening European security. *Space Policy* 9:65
- Hellenic Presidency's Initiative. "WEU Earth Observation Space Policy", SGS(98), Bruxelles, 27/2/1998, presented by Alexandros Kolovos, at the Space Group of WEU
- Holthoff H. A European satellite system-a cooperation programme for an autonomous European security policy, Second EUCOSAT Symposium on Satellite System for security: a European multi-user system, Bonn, 20 September 1995
- Kiernan V. Satellites play key role in swift Gulf Victory, *Space News*, March 4–10, 1991
- Kolovos A. The European space policy – its impact and challenges for the European security and defence policy. *ESPI perspectives* 27. European Space Policy Institute, September 2009, p 18. <https://espi.or.at/publications/voices-from-the-space-community/publications-of-the-former-espi-perspective-series/send/10-publications-of-the-former-espi-perspective-series/229-the-european-space-policy-its-impact-and-challenges-for-the-european-security-and-defence-policy>
- Lenzer C. WEU and Helios 2, Document 1525, Assembly of Western European Union, 14 May 1996. <http://aei.pitt.edu/53681/1/B0944.pdf>
- Lisbon Treaty (2009) Amending the Treaty on European Union and the Treaty establishing the European Community, signed at Lisbon, 13 December 2007
- Maastricht (1992) Treaty on the European Union signed at Maastricht on 7 February 1992. *Official Journal of the European Communities*, C 191
- McLean A (1995) Integrating European security through space. *Space Policy* 11(4):239–247
- Molard B (1998) How the WEU Satellite centre could help in the development of a European intelligence policy. In: Becher K, Molard B, Oberson F, Politi A (eds) *Towards a European intelligence policy*. Chaillot paper, 34. Institute for Security Studies of WEU, Paris
- Remuss L (2015) Responsive space. In: Schrogl K-U et al (eds) *Handbook of space security: policies, applications and programs*. Springer, New York
- Schrogl K-U et al (eds) (2015) *Handbook of Space Security: Policies, Applications and Programs*. Springer, New York [https://doi.org/10.1007/978-1-4614-2029-3\\_66](https://doi.org/10.1007/978-1-4614-2029-3_66)
- Space Policy. European cooperation in space-based defence, November 1991, p 337
- Voûte C, (1986) A European military space community. *Space Policy* 2(3):206–222
- WEU Council Of Ministers. European security: a common concept of the 27 WEU countries, Madrid, 14 November 1995, WEU. <http://www.weu.int/documents/951114en.pdf>
- WEU Council Of Ministers. Concept paper for the satellite centre. Paris, 13 May 1997
- WEU Council Of Ministers. Rome declaration, page. 10, para. 5, 16/11/1998
- WEU Satellite Centre. Feasibility of Satellite data reception at WEU, SC (97) 6, 1997
- WEU Satellite Centre. Mid-Term concept for improving access to satellite imagery, MTC/V.1.0/31.10.2000
- WEU Secretariat-General. WEU today. Brussels, January 2000. [http://www.weu.int/WEU\\_Today2.pdf](http://www.weu.int/WEU_Today2.pdf)



# Strategic Overview of European Space and Security Governance

# 23

Ntorina Antoni, Maarten Adriaensen, and Christina Giannopapa

## Contents

Introduction .....	422
National Level .....	423
France .....	425
Germany .....	427
Spain .....	428
Italy .....	429
United Kingdom .....	430
Multilateral Level .....	431
Archetype Model for National Space and Security Governance .....	442
Concluding Remarks .....	445
References .....	446

## Abstract

The importance of security is increasing in strategic policies, activities, and programs of European countries, the European Union (EU), and the European Space Agency (ESA). Each European country has a unique national space governance structure that facilitates linkages with the aforementioned and other space-related organizations. National space governance in this chapter means “the way that national authorities and structures are managed within a

---

N. Antoni (✉)  
Eindhoven University of Technology, Eindhoven, The Netherlands  
e-mail: [ntorina.antoni@gmail.com](mailto:ntorina.antoni@gmail.com)

M. Adriaensen · C. Giannopapa  
European Space Agency (ESA), Paris, France  
e-mail: [maarten.cm.adriaensen@gmail.com](mailto:maarten.cm.adriaensen@gmail.com); [christina.giannopapa@esa.int](mailto:christina.giannopapa@esa.int)

state in order to supervise space related organizations, space budget, space strategy and policy.” These structures determine decision-making power, representative mandates, implementation of programs, and interaction among all organizational actors. The chapter, thus, focuses on the governance structures that enable decision-making processes when it comes to space and security, within which there is ample attention for coordination among and between the national, multilateral, regional, and intergovernmental levels. The chapter concludes with an archetype model of national governance for space and security that facilitates interconnections with relevant organizations.

---

## Introduction

In Europe, the space sector is a particularly interesting and dynamic field, mainly because it includes several actors with varying priorities. Due to the inherent dual-use nature of space activities, responsibility for space has traditionally resorted under a state’s sovereign competences. Traditionally, security- or defense-related space programs have been kept at the national level or dealt with bilaterally or multilaterally in *ad hoc* cooperative programs. Only civilian space activities, including Earth observation, telecommunications, human spaceflight, space transportation, and technology development, have been the subject of cooperation at the regional and intergovernmental levels.

However, in the past years the security dimension of space activities has increasingly been coming to the attention of European countries, as well as the European Union (EU) and the European Space Agency (ESA). “Space and security,” both in its security *from* space and security *in* space form, is progressively contributing to the further integration of space activities in sectorial policies (Giannopapa et al. 2018). As such, countries conduct space and security activities at the national, multilateral, and intergovernmental levels, but also within EU and ESA contexts. The increasing security challenges the European countries and institutions are facing, together with the political momentum that is favorable for advancing Europe’s role in the field of security and defense, may lead to further integration covering the entire dual-use spectrum of space activities.

Europe has a long history of space integration for civil space activities, with tangible successes in the frame of ESA and the EU (Antoni et al. 2018). The rising challenges for Europe’s security have caused the EU and ESA to take a more active stance when it comes to security and defense, as elaborated in ► [Chap. 61, “Institutional Space Security Programs in Europe”](#) in Part 4 of the Handbook. It is noteworthy that in 2019, NATO, although with no operational capabilities of its own, adopted a space policy recognizing that space is essential to deterrence and defense. Simultaneously, European countries are increasingly recognizing the need for joint action to address societal challenges, including in the field of security and defense as described in ► [Chap. 25, “Space and Security Policy in Selected European Countries”](#) in Part 2 of this Handbook. The different nature and strategic objectives of all organizational actors involved in space and security in Europe lead

to a complex space and security governance. This raises challenges with regard to coordination among all actors that affect the governance of space security policy, activities, and programs.

Each European country has a unique national space governance structure responsible for overseeing space related organizations, space budget, space strategy and policy and implementation of space activities. This structure determines decision-making power, representative mandates, implementation of programs, and interaction between actors and stakeholders. The chapter focuses on selected number of countries with the largest space budgets, while considering interaction among the national, multilateral, and intergovernmental levels. In order to advance the understanding of the space and security governance, this chapter investigates the linkages whereof and based on the analysis of these governance structures, it concludes with an archetype model for national space and security governance.

---

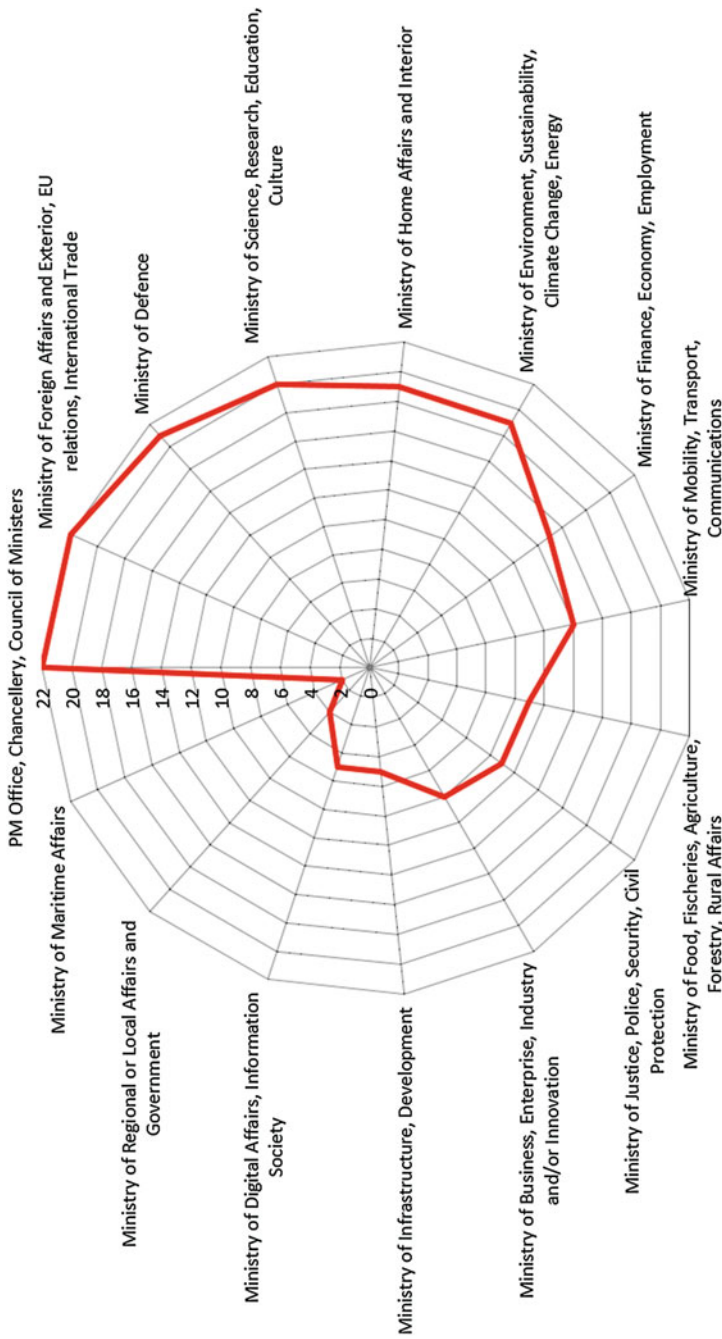
## National Level

All European countries have a specific governance structure to organize space- and security-related competences. In all selected ESA Member States, the Ministries of Foreign (and/or EU) Affairs, the Ministry or Ministries responsible for Science, Education and Research, and the Prime Minister's Office, Chancellery, or Council of Ministers are involved in space affairs. In almost all Member States, the Ministries of Defence are included in the national space governance (except for Luxembourg, where the competence for defense resides within the Ministry of Foreign and European Affairs).

A high number of Ministries of Home Affairs (Interior), Ministries of Justice and/or Security, and Ministries charged with environment, sustainable development and/or climate change (sometimes also energy, food, and/or agriculture) are involved in space affairs. This is due to the increasing role of space-based services in the areas of civil protection, crisis management, national security, sustainable development, climate change, and environmental affairs. Because of the importance of research and development (R&D), technology and innovation as well as economy and competitiveness, one or multiple associated ministries per Member State take up an important role of the national space governance.

The Ministry(-ies) competent for transport, infrastructure, telecom, and/or digital affairs are also increasingly active in space activities in the sub-domains of Global Navigation Satellite System (GNSS), Positioning, Navigation and Timing (PNT), Satellite Communication (SATCOM), frequency management, and integrated applications. Depending on the specific geographic location, policy-making approach and strategic priorities in space and other policy areas (for instance maritime or arctic), other Ministries are also involved in space affairs. On average between nine and ten Ministries per country (and not less than seven in the selected European countries) are involved in national space and security governance. Figure 1 below provides an overview of the types of Ministries involved in the national space and security governance.

Regardless of the number of Ministries involved in the national space- and security-related governance, one Ministry typically holds the main responsibility at



**Fig. 1** Ministries involved in space and security for selected European countries



the national level to define, coordinate, and/or implement a national space strategy, space policy, and space programs. Table 1 below provides an overview of the lead Ministries for the 22 ESA Member States.

Additionally, and as a result of the diverse competences that Ministries hold in space and security related areas, a wide variety of governmental bodies and agencies are involved therein. Each governance scheme of the 22 ESA Member States is inherently unique and based on historic remnants, strategic priorities, political compromise, national interests, and geopolitics. The following paragraphs provide some examples of space and security governance. In the following paragraphs, a representative sample of specific European countries is presented in order to show the unique approach followed across Europe in governing space security activities and programs.

## France

In France, CNES is the national space agency – a public administration organization with industrial and commercial purposes. CNES is charged with elaborating, proposing, and executing the French space program. CNES is under the joint supervision of the Ministry of Higher Education, Research and Innovation and the Ministry of the Armed Forces (CNES Website).

The Ministry of the Armed Forces is assisted by the *Chef d'état-major des armées* (French Armed Forces High Command), the *Direction générale pour l'Armement* (DGA) and the *Secrétaire Général pour l'Administration* (SGA) (Ministry of the Armed Forces 2017). DGA is the French Defence Procurement and Technology Agency. Within the DGA, the Security and Defence and Information Systems Service within the Security Operations and Information Systems Department and the Service for Preparation of Future Systems and Architecture in the Strategy Directorate (DGA/DS/SPSA/CISR) are responsible for space. DGA, on behalf of the Ministry of Armed Forces, exercises the guardianship over CNES (Ministry of the Armed Forces 2018).

CNES proposes the French space policy under the responsibility of the Minister for Higher Education, Research and Innovation and has a special partnership with the Ministry of the Armed Forces for what concerns military space activities (CNES Website). CNES conducts research and technology for future programs that respond to military needs. DGA delegates the management for military space programs to CNES, and DGA may contribute to the financing of dual-use satellites procured by CNES. Given the dual-use of space assets and the importance of space, and the general acceptance of the use of military capabilities for civilian objectives in France, the French DGA and the General Staff work closely with CNES. The CNES Centre d'Orbitographie Opérationnelle (COO) at Toulouse is the CNES operational orbit tracking center. Coordination of the CNES Defence Team is done by a military advisor (CNES 2017).

The Space Committee and the Interparliamentary Group for Space have further contributed to the French space and security governance. The Space Committee,

**Table 1** Coordinating entity and ministries competent for space affairs. (Source: ESA (2017) with updates)

ESA Member State	Coordinating entity	Ministries competent for space affairs
Austria	Austrian Research Promotion Agency (FFG)	Ministry for Transport, Innovation and Technology
Belgium	Belgian Science Policy Office (BELSPO)	State Secretary charged with Science Policy
Czech Republic	Department of Space Activities and R&D	Ministry for Transport
Denmark	Danish Agency for Higher Education and Science	Ministry of Higher Education and Science
Estonia	Estonia Space Office, Enterprise Estonia	Ministry for Economic Affairs and Communications
Finland	Finish Funding Agency for Innovation	Ministry of Economic Affairs and Employment
France	National Centre for Space Research (CNES)	Ministry of Higher Education, Research and Innovation
Germany	German Aerospace Centre (DLR)	Ministry for Economic Affairs and Energy
Greece	5G, Wireless and Space Department	General Secretariat for Telecommunications and Post
Hungary	Department for Space Research and Space Activity	Ministry of Foreign Affairs and Trade
Ireland	Enterprise Ireland	Department of Business, Enterprise and Innovation
Italy	Italian Space Agency (ASI)	Prime Minister/Council of Ministers
Luxembourg	Luxembourg Space Agency	Ministry of Economy
The Netherlands	Netherlands Space Office (NSO)	Ministry of Economic Affairs and Climate
Norway	Norwegian Space Centre (NSC)	Ministry of Industry, Trade and Fisheries
Poland	Space Policy Unit, Innovation Department	Ministry of Economic Development
Portugal	Space Office, Foundation for Science and Technology (FCT)	Ministry of Education and Science
Romania	Romanian Space Agency (ROSA)	Ministry of Research and Innovation
Spain	Centre for the Development of Industrial Technology (CDTI)	Ministry of Economy and Enterprise
Sweden	Swedish National Space Agency (SNSA)	Ministry of Education and Research
Switzerland	Swiss Space Office	State Secretariat for Education, Research and Innovation
United Kingdom	UK Space Agency (UKSA)	Department for Business, Energy and Industrial Strategy

which was established in 1989, is a Committee with representatives from various institutions and bodies charged with the objective of converging to assure the coherence of the national space policy by: analyzing multiannual civil and military space plans and preparing government decision on space policy; assessing the influence of space programs on French and European industry; preparing French position on international cooperation on space activities; and proposing to the prime minister any necessary action. The Committee is composed of representatives from various Ministries and government bodies (Legifrance 1989). Established in 1994, the Interparliamentary Group for Space was renamed the Group of French Elected for Space in 2016, composed of national, regional, and local level representatives that are involved in space activities (GPE Website).

Furthermore, the Ministry of Foreign Affairs plays a key role in space and security governance. Within the Ministry, both the Directorate-General for Political Affairs and Security, the Directorate-General for Globalisation, Culture, Education and International Development, and the Directorate for European Affairs are involved in contributing to space and security activities. In addition to the links established between the Ministries and Implementing Entities, on the one hand, and international/supranational bodies on the other hand, the Ministry of Foreign Affairs is directly involved in the representation of France in international and supranational bodies, for instance through the Permanent Representation to the EU in Brussels. As such, it complements the representation of specific to the Ministry stakeholders.

## Germany

In Germany, the Ministry for Economic Affairs and Energy (BMWi) is mainly responsible for Germany's civilian space activities, whereas the Ministry of Transport and Digital Infrastructure (BMVI) oversees selected European Union flagship programs Galileo and Copernicus. The Foreign Office is also active in the space and security realm, as it contributes to international space law discussions. The Ministry of Defence (BMVg) operates Germany's reconnaissance satellites, while the Chancellery oversees the intelligence service (BND) and the Ministry of the Interior (BMI) coordinates the protection of critical infrastructure and national crisis management (Governance Post 2017; BMWi Aerospace Policy). The Federal Government Coordinator of German Aerospace Policy coordinates the Federal Government's measures to strengthen the international competitiveness of Germany's aerospace sector in the fields of research and development (BMWi Aerospace Policy). In addition to the links established between the Ministries, the Government Coordinator and the Implementing Entities, on the one hand, and international and supranational bodies, on the other hand, the Ministry of Foreign Affairs is directly involved in space matters as it often represents Germany in international and supranational bodies.

Within the federal government, the Ministry of Transport and Digital Infrastructure (BMVI) has the lead responsibility for the Copernicus program. The Ministry is

responsible for the German participation in the program design vis-à-vis the European Commission and other European players. BMVI is also responsible for the provision of public funds for the German contribution to the Copernicus programs of ESA and EUMETSAT. At the national level, BMVI coordinates the required national accompanying measures related to the programs. Other Ministries, including the Ministry of Defence, also contribute to the Federal Government's positioning. In cooperation with the other Federal Ministries involved, BMVI regularly develops a cross-departmental program where the activities of the Federal Government are defined. The DLR Space Administration monitors the Copernicus Programme on behalf of BMVI. The DLR Space Administration also supports information and public relations activities in Germany for its citizens. As a project management agency to which statutory powers have been transferred, it carries out support measures relating to Copernicus on behalf of the Federal Government. According to its responsibility for implementing the National Programme for Space and Innovation, DLR establishes appropriate linkages between Copernicus and national missions and activities on behalf of the BMWI (BMVI 2017).

The Deutsches Zentrum für Luft- und Raumfahrt (DLR) is the national space agency. It reports directly to the BMWi. DLR was founded in 1969 through the merger of several institutions. Acting on behalf of the Federal Government, DLR Space Administration designs and implements Germany's Space Program, which integrates all German space activities on the national and European level. These activities include Germany's national Space Program and Germany's contributions to ESA and EUMETSAT. In addition, the DLR shapes and monitors the space topic within the European Framework Programme for Research and Innovation. The DLR's principal client is the Federal Ministry for Economic Affairs and Energy. However, the DLR also works for other ministries, mainly in application-related fields such as earth observation, navigation, and satellite communication (DLR Website, BMVI 2017).

## Spain

In Spain, the Ministry of Economy and Enterprise (Ministerio de Economía y Empresa) is charged with drafting and implementing government policy on economic matters and reforms to improve competitiveness, industrial development, telecommunications and information society, development of the Digital Agenda as well as the policy of support for the economy and enterprises (Spanish Government 2018). The Ministry has the main responsibility for space affairs in Spain.

Resorting under the Ministry of Economy and Enterprise, the Centre for the Development of Industrial Technology (CDTI) created in 1977 is a public entity which promotes innovation and technological development in Spain. The CDTI manages the space budget for R&D projects and contributes to the improvement of the technological level of the industry at national and international level. Within CDTI there is a dedicated Directorate of European Programmes, Space and Technological Returns that is in charge of liaising with the Copernicus program (CDTI

Website). The CDTI is involved with the Ministry of Defence through agreements in place with the DGAM (Directorate General of Armaments and Material) and Isdefe (Engineering Systems for the Defence of Spain) (CDTI 2011). The CDTI has been supported by the Ministry of Defence to coordinate various aspects of the Spanish participation in the EU SST Consortium and direct interaction with ESA to coordinate the transfer of those aspects related to security and confidential information to its SSA program (Spanish Ministry of Defence 2015, 2017). The Spanish Space Surveillance and Tracking (S3T) system is managed by CDTI (CDTI 2018).

The Interministerial Commission of Industrial and Space Policy constituted in November 2014 has as objective to enhance the existing coordination among the ministerial departments that participate well as promoters or users of space systems or that manage Spanish participation in international organizations such as ESA, EUMESAT, or the EU. This Interministerial Commission was charged in 2015 with preparing the Agenda 2020 of the Spanish space sector, a strategic national planning for space, which was anticipated, which could lead to the establishment of a Spanish Space Agency (Infoespacial 2015).

## Italy

Responsibility for space activities has recently been put directly under the supervision of the Prime Minister. The Italian Parliament approved on December 22, 2017, the new space governance law, mandating the establishment of an Inter-ministerial Committee for Space and Aerospace Research Policies, and the President of ASI reporting directly to the Prime Minister's Office. The Law entered into force on February 25, 2018. The Committee is chaired by the President of the Council of Ministers, or by the Undersecretary of State to the Presidency of the Council of Ministers with responsibility for Space and Aerospace Policies, and is composed of the Ministers of Defence, the Interior, Cultural Heritage and Activities and Tourism, Agricultural, Food and Forestry Policies, Education, University and Research, Economic Development, Infrastructure and Transport, Environment and Protection of Land and Sea, Foreign Affairs and International Cooperation, and Economy and Finances, as well as the President of the Conference of Presidents of the Regions and Autonomous Provinces and the President of the ASI (Altalex 2018).

The Italian Space Agency (ASI) is the national public body tasked with promoting, developing, and disseminating scientific and technological research applied to the space and aerospace field, and coordinating and managing national projects and Italian participation in European and international projects in accordance with the government's guidelines as promoted by the Inter-ministerial Committee for related policies space and aerospace research, in the framework of the coordination of international relations assured by the Ministry of Foreign Affairs, taking care to maintain the competitiveness of the Italian industrial sector. ASI reports to the Ministry of Education, University and Research, without prejudice to the powers expressly assigned to the Inter-ministerial Committee (Altalex 2018).

The main players concerned in military exploitation of space are the Stato Maggiore Difesa (SMD, the Joint Defence Staff organisation), the Direzione Nazionale Armamenti (SGD/NAD, National Armaments Directorate), and the Air Force service (IAI 2003).

## United Kingdom

The Department for Business, Energy and Industrial Strategy (BEIS) is the parent department of the UK Space Agency. It has the lead for space affairs in the UK. The Minister of State for Universities, Science, Research and Innovation is the responsible minister for space activities in the UK. He is reporting to both BEIS and the Department of Education. BEIS uses satellite data for more accurate mapping through the Ordnance Survey; it also monitors land use through the work of the Land Registry; it delivers space weather and weather forecasting through the Met Office; it coordinates resilience to space weather; and it is in charge of export control (UK Government 2015). Resorting under BEIS, the UK Space Agency helps to bring together UK civil and commercial space programs and interests. It is an executive agency of the Department for Business, Energy and Industrial Strategy and is responsible for all strategic decisions on UK civil space programs. It supports UK space industry initiatives and licenses the launch and operation of all UK satellites, both military and nonmilitary, and has regulatory responsibilities under the 1986 Outer Space Act. It promotes cooperation through participation and contribution to the European Space Programme, and other European initiatives. UKSA represents the UK at ESA. Given the dual-use of space assets and the importance of space, the UK Ministry of Defence works very closely with the UK Space Agency (UK Ministry of Defence 2017).

UK military space capabilities are primarily coordinated and delivered by the Royal Air Force and Joint Forces Command (UK Ministry of Defence 2017). The Ministry of Defence uses satellite services space-enabled services in support of global military operations, from disaster relief response to the employment of precision weapons. The Home Office uses space-enabled capabilities for critical emergency services and law enforcement activities. The National Space Policy clearly articulates cross-government reliance on space-enabled capabilities. From a military perspective, the Royal Air Force (RAF) is recognized as the most significant contributor to space operations, since it retains most of the UK's military space expertise and manages key UK space capabilities (UK Ministry of Defence 2017).

The Foreign and Commonwealth Office is directly involved in the representation of the UK in international and supranational bodies, for instance through the Permanent Representation to the EU in Brussels. The Foreign and Commonwealth Office assists the space sector in capturing new export opportunities. It also facilitates the representation of UK policy in international civil and security partnerships, such as through the United Nations (UK Government 2015).

The Cabinet Office is a key stakeholder of the National Space Security Policy. Its main task is the coordination and management of satellite data for emergency response (UK Government 2018).

---

## Multilateral Level

Moving from the national level to the multilateral level allows to investigate the precise linkages in place between the national authorities representing European countries and the international organizations, initiatives, and *fora* in space, security, and defense. This is an established approach in Europe to develop and acquire high-quality space systems, based on collective needs, pooling of resources, and cost sharing. ESA Member States largely adhere to international legal and regulatory regimes in the field of space, security, and defense. Table 2 below provides an overview of relevant international treaties and initiatives in space and security.

Because of the nature and strategic importance of space, security, and defense activities, European countries are involved in a large variety of international organizations. Every state is represented in a variety of international organizations, international initiatives, and bilateral/multilateral cooperation fora, as presented in Table 3. The latter provides an overview of all relevant space, security, and defense organizations and the level of participation of the 22 ESA Member States. This extensive, yet non-exhaustive list demonstrates the broad range of European and international cooperation in the field of space, security, and defense. Based on the data collected for each European country, this study was able to identify trends on the role of national authorities that are involved in space and security or defense activities.

Each state is represented by the most relevant Ministry or Ministries in the various space and security related organizations. For instance, a Ministry charged with Environment, Sustainable Development and/or Climate Change often represents their respective state in the European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT) and in the European Centre for Medium-Range Weather Forecasts (ECMWF). With regard to ESA and Copernicus/Galileo programs, the Ministries that generally participate are usually those of Education and Science, Transport and Innovation and Ministries of Economy and Trade. For the International Telecommunications Union (ITU) the responsibility typically lies with the Ministry of Transport, Telecom and/or Digital Affairs. The Ministries of Defence have the lead in defense-related organizations, such as the European Defence Agency (EDA), the North Atlantic Treaty Organization (NATO), and the European Union Satellite Centre (SatCen). The Ministry of Foreign (and/or EU) Affairs has the lead role when it comes to space-, security-, and defense-related cooperation with UN-related bodies such as the UN Committee on the Peaceful Uses of Outer Space (COPUOS). For the International Civil Aviation Organization (ICAO), the European























Union Aviation Safety Agency (EASA), and Eurocontrol, the national agency for civil aviation is the most relevant.

In addition to international cooperation in space and security effected through representation in international organizations, there is a considerable number of initiatives and cooperation taking place at the bilateral and regional levels as seen in Table 3. In this context, and in order to exemplify what types of cooperation take place between European countries, this chapter will take a closer look at a few of these international initiatives and cooperation *fora*. First the Franco-German and Franco-Italian cooperation are addressed as examples of an integrated approach to space, security, and defense at the bilateral level.

The Treaty on Franco-German Friendship (known as the Élysée Treaty), signed on January 22, 1963, by German Federal Chancellor Adenauer and France's General de Gaulle, is the symbol of the relationship forged between France and Germany (France Diplomatie Website). More recently, in the margins of the 19th Franco-German Ministerial Council that took place in July 2017, the French and German Heads of State agreed in the Franco-German Security and Defence Council (CFADS). Through this, they render available the satellite imagery from the French high resolution *Composante Spatiale Optique* (CSO) and the German SARah reconnaissance satellites to the EU Satellite Centre (Satcen) and open the door to partnership with other EU member states. Moreover, France and Germany coordinate their efforts in military Earth Observation. Both countries have called for high security requirements for Galileo, with the objective of ensuring European strategic autonomy for military applications and in order to enhance the international credibility of Galileo (Defense aerospace 2017). During the Meseberg Summit on June 19, 2018 (20th Franco-German Ministerial Council), France and Germany agreed to launch a working group with the task of making reports for the EU that address new challenges in space politics and economics (NewSpace in particular). In the field of launchers, the countries reaffirmed their full support for the ESA Ariane 6 program (Meseberg 2018).

France and Italy enjoy active space collaboration, as reflected by annual summits organized since 1982. In the September 2017 Franco-Italian summit, both countries committed to reinforce their cooperation in space, for example through the development of dual-use technologies and through the identification of opportunities for the next generation of Earth observation and satellite communication satellites. It was agreed to put CSO and COSMO Skymed imagery at the disposal of the European External Action Service (EEAS). Cooperation on Multinational Space-based Imaging System (MUSIS) also continues. France and Italy will update the intergovernmental agreement with which they joined activities since 2007. The governments have mandated CNES and ASI, respectively (Elysee 2017). In addition, the third phase of the SICRAL (*Sistema italiano per comunicazioni riservate e allarmi*) is conducted in cooperation between Italy and France. SICRAL became operational after April 2015 with the launch of SICRAL 2, with an estimated operational life span of 15 years. SICRAL 2 is a geostationary satellite able to enhance the capability of military satellite communications already offered by SICRAL 1 and SICRAL 1B and by France's Syracuse System. SICRAL 2 supports

satellite communications for the Italian and French Armed Forces, anticipating the needs of growth and development in the next few years. The satellite has an additional backup function to the French Syracuse 3 system and that of SICRAL 1B allocated to NATO communications (Telespazio Website).

Furthermore, there are a number of regional cooperation initiatives that deal with space and defense in Europe. For example, the Five Eyes community (FVEY) brings the United Kingdom, the United States, Canada, Australia, and New Zealand into the world's most complete and comprehensive intelligence alliance. The alliance is also involved in the "aerospace domain" which covers ballistic missile tests, foreign satellite deployments, and the military activities of relevant air forces (UK Defence Journal 2017). In addition, during World War II, the USA developed foreign SIGINT relationships with the United Kingdom and the Dominions of Canada, Australia, and New Zealand. FVEY was originally founded through the signature of the Britain–United States of America (BRUSA) agreement for co-operation in Signals Intelligence (SIGINT), now known as the United Kingdom–United States of America (UKUSA) Agreement, on March 5, 1946. SIGINT capability is space-based, including satellites used for military missions such as earth observation and reconnaissance satellites, electronic signals intelligence satellites, and civil and military communications satellites (Pfluke 2019). The Agreement consolidated the Special Relationship between Britain and the United States. FVEY expanded to also include Canada in 1948 and Australia and New Zealand in 1956. The SIGINT surveillance program was originally known as ECHELON (UK Defence Journal 2017; Lawfare 2019). The FVEY co-operation with Denmark, France, Norway, and the Netherlands is known under the name "Nine Eyes." Additionally, there is the SIGINT Seniors Europe (SSEUR) also known as "Fourteen Eyes" which consists of "Nine Eyes" plus Belgium, Germany, Italy, Spain, and Sweden. SSEUR's primary objective is to coordinate the exchange of military signals amongst its members. NATO Members have additional intelligence cooperation links (UK Defence Journal 2017). Furthermore, the Berne Club is a cooperation framework among Western European internal security services. It is based on periodic meetings attended by the heads of the European Intelligence Services. The Berne Club operates in an informal way (Nomikos 2014).

---

## Archetype Model for National Space and Security Governance

Based on the research on the selected ESA Member States, the organization of space- and security-related activities in countries is multifaceted. The governance of space and security mainly depends on three factors: (1) the applications of space-based assets and services in the fields of Earth observation (EO), Positioning, Navigation and Timing (PNT), Satellite Communications (SATCOM), Space Situational Awareness (SSA), (2) the involvement of a wide variety of involved Ministries based on national competences related to space and security, and (3) the level of programs at the national, multilateral, and intergovernmental levels. National space strategies contribute to this multifaceted nature of space- and security-related activities. Security and Defence applications of space activities (security *in* space and security *from*

space) are becoming increasingly important. Both the incorporation of security and defense as a priority in national space strategies and the development of dedicated space security or space defense strategies reflect the increase of this importance. As a result of the increasing importance of security and defense in space, the role of national ministries and agencies, tasked with security and defense activities in national space governance, is gradually increasing. Besides the ministries that traditionally held responsibility for space activities (most often the Ministry of Science, Education and Research or the Ministry of Economy and/or Industry and Innovation), the Ministries of Defence, Foreign Affairs, Home Affairs, Justice and/or Security, and the Prime Minister's Office or Chancellery have an increasingly important role in space governance at all levels.

Figure 2 provides an archetype of space and security governance. It was generated based on recurrent patterns, correlation between ministries, implementing entities, and respective space-related competences of all governance schemes for each ESA Member State and the linkages to space and security relevant organizations. The model reflects the relevance of security and defense actors in national space governance and the observed role of specific Ministries and Implementing Agencies (governmental bodies) in the definition of national space strategy and policy and in the programmatic implementation of space activities. Although space and security governance is inherently unique for each member state, the model in Fig. 2 shows which entities are typically involved in the space and security governance landscape. Because of the increasing role of security and defense applications in space, the Ministry of Defence, the Ministry of Home Affairs, and the Ministry of Foreign Affairs play a crucial role. Their respective roles also imply increasing participation of the national defense procurement agency, the military general staff, defense research agencies, and national intelligence services, both internal, foreign, and military. National civil protection and crisis management services can increasingly benefit from the use of space-based assets and services. The Ministry of Foreign Affairs plays an indispensable role in the context of bilateral, multilateral and supranational space programs (including ESA, EU, and NATO). Although it is primarily the national space agencies that represent their member states at/in ESA, the countries' Ministries of Foreign Affairs are becoming increasingly active (directly) at the ESA Council level and delegate body level. This is because of the increasing strategic importance of space- and security-related activities. As a matter of fact, in an increasing number of countries it is the highest level of government that is involved in space activities, as reflected by the role of the Prime Minister's Office, the national Chancellery, the Council of Ministers, or the Ministry of General Affairs.

As space-based assets and services can be of great help in combating climate change, in furthering sustainable development and in protecting the environment, most member states directly involve the ministries responsible for those competences in the space decision making and implementing landscape. Very often (but not exclusively) the same ministries are also charged with supervision of the national meteorological institute. The national meteorological institutes depend on space-based assets and services and as such often represent their country in the frame of EUMETSAT and ECMWF. The ministry or ministries competent for transport,

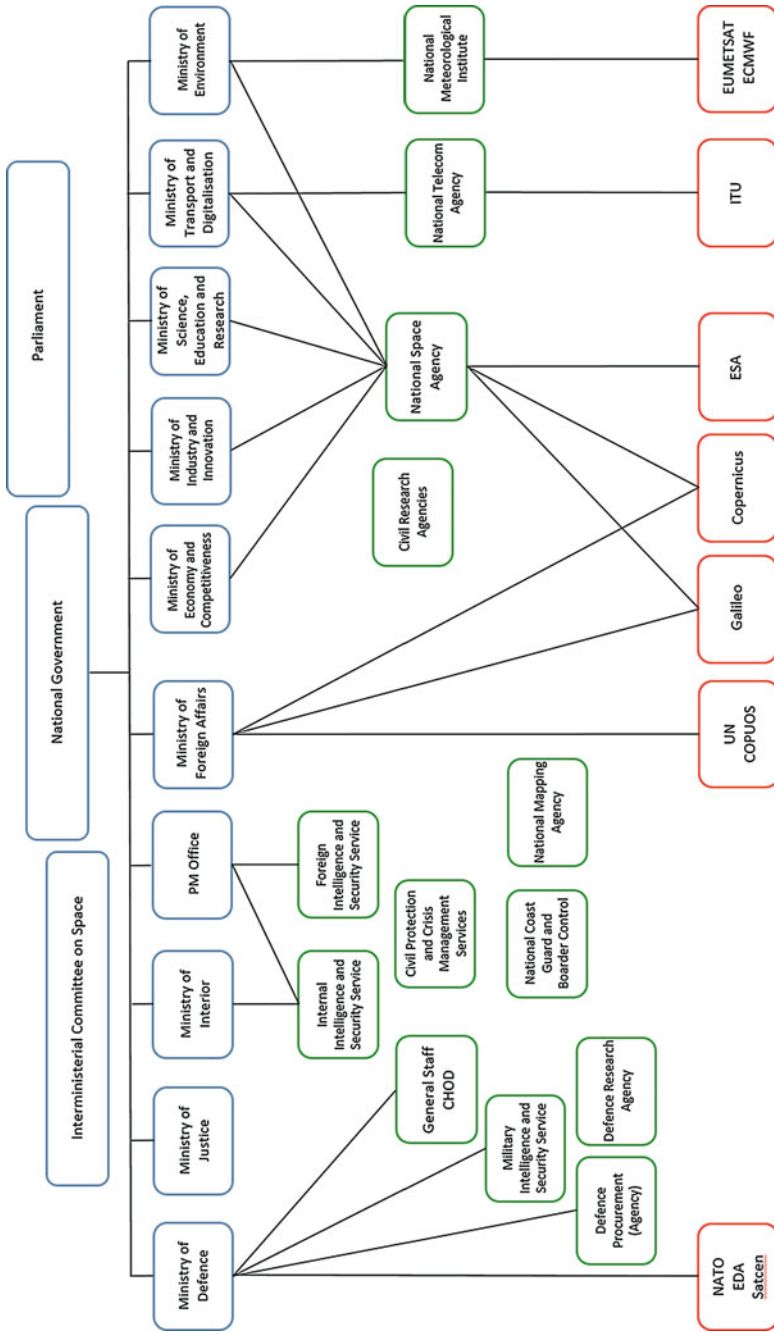


Fig. 2 Archetype space and security governance model (generated based on recurrent patterns of all governance schemes of ESA Member States)

infrastructure, telecom, and/or digital affairs are also increasingly active in space activities. The national telecom agencies, acting under the respective responsible ministry, often represent their country in the frame of the International Telecommunications Union. Space will continue to be an important economic sector, not in the least because of its highly skilled workforce and the innovation that takes place. Depending on the member state, one or more Ministries that are tasked with economic and trade-related subjects, such as competitiveness, enterprise, industry, technology, and/or innovation are therefore directly involved in developing and executing space activities. The Ministries of Science, Education and Research have been involved in space affairs from the very onset of space activities in Europe. For that reason, national space agencies have often been under the direct supervision of the ministry or ministries charged with science, education, and research.

Responsible space entities increasingly respond to the needs of multiple ministries. Multiple funding sources come from different Ministries, increasing the need for coordination of space affairs at the level of the Prime Minister's Office, Chancellery, or Council of Ministers, or the joint supervision by multiple Ministries. This reflects the diversity of Ministerial interests in space activities and applications. Various national (civil or dual-use) research entities are involved in space affairs, as such complementing the role of national space entities. The national mapping entities (or national geo-data or geo-information agencies or cadaster agencies or geographical institutes) increasingly depend on space-based data and provide crucial services for a multitude of Ministries and governmental bodies. In the frame of national security, coast guards and national border protection agencies also increasingly rely on space-based services in the execution of their mandate.

---

## Concluding Remarks

Europe has been taking a more active stance in the field of foreign affairs and security and defense. Member states are increasingly recognizing the need for joint action to address societal challenges together, including in the field of security and defense. Space integration in Europe for civilian uses has a long track record and has demonstrated tangible successes in the frame of ESA and the EU. Contrary to civil space activities, security-related space activities traditionally took place at the national level, or via bi- or multilateral basis. The increasing security challenges the European countries are facing, together with the political momentum favorable for advancing the EU role in the field of security and defense, may lead to further integration covering the entire dual-use spectrum of space activities.

This chapter provides evidence of the increasing importance for security and defense in national space strategy and policy, with an emphasis on the role of international cooperation. This trend runs parallel with an increasing interest in space affairs of Ministries with security- and/or defense-related competences. The participation of the various ministries in space- and security-related international organizations shows that Ministries of Defence are becoming increasingly important stakeholders for national space strategy and resulting programmatic activities. The

increasing use of space-based services for civil protection, crisis management, and border control further strengthen the need for participation of the Ministry or Ministries responsible for Home Affairs, Justice and/or Security in the frame of national space policy, governance, and programs. Ministries charged with Environment, Sustainable Development and Climate Change as well as Ministries charged with Transport, Infrastructure, Development, Telecom and Digital Affairs are important user Ministries, fully benefiting from space-based services and applications. Because of the strategic importance of space, security, and defense, the highest national political level is directly involved in space affairs through the PM Office, Chancellery, and/or Council of Ministers.

**Disclaimer** The contents of this chapter and any contributions to the Handbook reflect personal opinions and do not necessarily reflect the opinion of the European Space Agency (ESA).

---

## References

- Altalex (2018) Misure per il coordinamento della politica spaziale e aerospaziale e disposizioni concernenti l'organizzazione e il funzionamento dell'Agenzia spaziale italiana, Legge, 11/01/2018 n° 7, G.U. 10/02/2018, 14 February 2018. Available at: <http://www.altalex.com/documenti/leggi/2018/02/14/misure-per-il-coordinamento-dellapolitica-spaziale>
- Antoni N, Adriaensens M, Papadimitriou A, Giannopapa C, Schrogl KU (2018) Re-affirming Europe's ambitions in space: past, present and future perspectives. *Acta Astronaut* 151:772–778
- BMVI (2017) The Copernicus Strategy of the German Federal Government Copernicus for Germany and Europe –the Federal Government's strategy and fields of action for successful implementation of the European Earth Observation Programme, 13 September 2017
- CDTI (2011) Spanish strategy for ESA and EU Space programmes “HISNORSAT: encuentro de la industria especial Hispano-Noruega” Jorge Lomba, Jefe del Departamento de industria de la ciencia y el espacio, 3 May 2011. Available at: [https://www.cdti.es/recursos/doc/Programas/Aeronautica\\_espacio\\_retornos\\_industriales/Espacio/29437\\_101110112011135137.pdf](https://www.cdti.es/recursos/doc/Programas/Aeronautica_espacio_retornos_industriales/Espacio/29437_101110112011135137.pdf)
- CDTI (2018) Perspectiva CDTI, ESPACIO|Los datos europeos recibidos en el #S3TOC de @CDTIoficial predicen que la reentrada de la estación orbital china #TIANGONG-1 se producirá el 1 de abril de 2018, 28 March 2018. Available at: <http://perspectivacdti.es/espacio-los-datos-europeos-recibidos-en-el-s3toc-de-cdtioficial-predicen-que-lareentrada-de-la-estacion-orbital-china-tiangong-1-se-producira-el-1-de-abril-de-2018/>
- CDTI Website. About CDTI, organizational structure, Comité de Dirección Available at: <https://www.cdti.es/index.asp?MP=6&MS=801&MN=3#Juan%20Carlos%20Cort%C3%A9s>
- CNES (2017) CNES organisation chart, 30 November 2017. Available at: <https://cnes.fr/en/cnes-organization-chart>
- CNES Website. Organigramme du CNES. Available at: <https://cnes.fr/fr/organigramme-du-cnes>
- Defense aerospace (2017) Meeting of the French-German Defense and Security Council: conclusions (excerpt), 14 July 2017. Available at: [http://www.defense-aerospace.com/articles-view/verbatim/4/185306/conclusions-of-franco\\_germandefense-council.html](http://www.defense-aerospace.com/articles-view/verbatim/4/185306/conclusions-of-franco_germandefense-council.html)
- DLR Website. DLR space administration. Available at: [http://www.dlr.de/rd/en/desktopdefault.aspx/tabid-2099/3053\\_read-4706/](http://www.dlr.de/rd/en/desktopdefault.aspx/tabid-2099/3053_read-4706/)
- Elysee (2017) Sommet Franco-Italien, 27 September 2017, Lyon. Available at: <http://www.elysee.fr/assets/SommetFrancoItalien-FR.pdf>
- ESA (2017) European Space Agency Council, ESA Member States Strategies and Plans – Countries Overview Information Document, Paris 12 October 2017

- France Diplomatie Website. France and Germany, Elysée Treaty. Available at: <https://www.diplomatique.gouv.fr/en/country-files/germany/france-and-germany/elysee-treaty/>
- French Ministry of the Armed Forces (2017) Ministère des Armées, Organigramme simplifié du ministère des Armées, 7 June 2017. Available at: <http://www.defense.gouv.fr/portail/ministere/organisation-du-ministere-des-armees/organisation-duministere-des-armees/organigramme-simplifie-du-ministere-des-armees/organigramme-simplifie-duministere-des-armees>
- French Ministry of the Armed Forces (2018) Ministère des Armées, L'organigramme de la DGA, 19 January 2018. Available at: <https://www.defense.gouv.fr/dga/ladga2/organisation/l-organigramme-de-la-dga>
- Giannopapa C, Adriaensen M, Antoni N, Schrogl KU (2018) Elements of ESA's policy on space and security. *Acta Astronaut* 147:346–349
- Governance Post (2017) After the Election, Germany's Space Policy Must Take Shape, 13 December 2017. Available at: <https://www.hertie-school.org/the-governance-post/2017/12/election-germanys-space-policy-must-takeshape/>
- GPE Website. Le GPE. Available at: <http://www.gpespace.fr/spip.php?article1>
- IAI (2003) Space and Security Policy in Europe, November 2003, ESA Study. Available at: [http://www.iai.it/sites/default/files/2003\\_space-and-security-in-europe.pdf](http://www.iai.it/sites/default/files/2003_space-and-security-in-europe.pdf)
- Infoespacial (2015) Hacia la creación de una Agencia Espacial Española, 15 December 2015. Available at: <http://www.infoespacial.com/ie/2015/12/15/opinion-agenda-sector-espacial-espana.php>
- Lawfare (2019) Newly Disclosed NSA Documents Shed Further Light on Five Eyes Alliance, 25 March 2019. Available at: <https://www.lawfareblog.com/newly-disclosed-nsa-documents-shed-further-light-five-eyes-alliance>
- Legifrance (1989) Décret n°89-508 du 19 juillet 1989 portant création du comité de l'espace, [https://www.legifrance.gouv.fr/affichTexte.do?sessionId=83D1F8EC5C8C56E062B8C8C80DB63E0A.tpdjo12v\\_1?cidTexte=JORFTEXT00000699675&idArticle=&dateTexte=20101206](https://www.legifrance.gouv.fr/affichTexte.do?sessionId=83D1F8EC5C8C56E062B8C8C80DB63E0A.tpdjo12v_1?cidTexte=JORFTEXT00000699675&idArticle=&dateTexte=20101206)
- Meseberg (2018) Meseberg Declaration, Renewing Europe's promises of security and prosperity, 19 June 2018. Available at: <https://archiv.bundesregierung.de/archiv-de/meta/startseite/meseberg-declaration-1140806>
- Nomikos M (2014) European Union intelligence analysis Centre (INTCEN): next stop to an agency. *J Mediterr Balkan Intell* 4(2), December 2014
- Pfluke C (2019) A history of the five eyes Alliance: possibility for reform and additions. *Comp Strateg* 38(4):302–315
- Spanish Government (2018) Official State Journal, 7 June 2018. Available at: <http://www.boe.es/boe/dias/2018/06/07/pdfs/BOE-A-2018-7575.pdf>
- Spanish Ministry of Defence (2015) Ministerio de Defensa, D.G.A.M. Plan Director de Sistemas Espaciales, p.5, July 2015. Available at: <http://www.defensa.gob.es/Galerias/dgamdocs/plan-director-sistemas-espaciales.pdf>
- Spanish Ministry of Defence (2017) Programa SST/S3T, October 2017. Available at: [http://www.defensa.gob.es/Galerias/dgamdocs/programa-SST\\_S3T.pdf](http://www.defensa.gob.es/Galerias/dgamdocs/programa-SST_S3T.pdf)
- Telespazio Website. SICRAL. Available at: <http://www.telespazio.com/programmes-programmi/sicral>
- UK Defence Journal (2017) UKDJ, The Five Eyes – The Intelligence Alliance of the Anglosphere, 14 November 2017. Available at: <https://ukdefencejournal.org.uk/the-five-eyes-the-intelligence-alliance-of-the-anglosphere/>
- UK Government (2015) National Space Policy, December 2015. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/484864/NSP\\_-\\_Final.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/484864/NSP_-_Final.pdf)
- UK Government (2018) Legislation – Space Industry Act 2018. Available at: <http://www.legislation.gov.uk/ukpga/2018/5/contents/enacted/data.htm>
- UK Ministry of Defence, Joint Doctrine Publication 0–30 (JDP 0–30) – UK Air and Space Power, 2nd edn, December 2017, 113. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/668710/doctrine\\_uk\\_air\\_space\\_power\\_jdp\\_0\\_30.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668710/doctrine_uk_air_space_power_jdp_0_30.pdf)



# European Space Security Policy: A Cooperation Challenge for Europe

# 24

Jean-Jacques Tortora and Sebastien Moranta

## Contents

Introduction .....	450
Prospects for a European Space Security Policy .....	452
Stakes Are High for Europe and Will Continue to Increase .....	452
Socioeconomic Rationale and Service-Oriented Policy .....	452
European Autonomy and Weight on the International Scene .....	453
Europe Is Mobilizing But Follows an Approach That Is Called to Evolve .....	456
Accommodating Different Concerns and Interests: Achievements and Limits .....	459
Space Traffic Management: A Coordination and Leadership Challenge .....	461
Conclusions .....	463
References .....	464

## Abstract

Experts consensually agree that ensuring the security, safety, sustainability, and stability of space activities is a growing challenge and therefore a dominant concern for public and private stakeholders worldwide. At the crossroad of multiple strategic, political, and operational issues, space security also holds a special place in the European context. This chapter reviews major policy stakes for Europe in this field and discusses the achievements and limits of the current approach to space security in Europe. In particular, it examines some recent developments in the space security field such as the major steps announced by the US government in the field of space traffic management and its potential consequences on the ongoing progress of the European agenda in this matter.

J.-J. Tortora · S. Moranta (✉)

European Space Policy Institute (ESPI), Vienna, Austria

e-mail: [Jean-Jacques.Tortora@espi.or.at](mailto:Jean-Jacques.Tortora@espi.or.at); [sebastien.moranta@espi.or.at](mailto:sebastien.moranta@espi.or.at)



## Introduction

Although sometimes perceived as slow paced and resistant to change, space is actually a fast-changing sector, both at the industry and policy level. Shaped by 60 years of constant governmental efforts in a tense geopolitical context, space has expanded toward privately owned initiatives to become not only a decisive item on governments' agenda but also an area of interest for private companies, entrepreneurs, and investors. In this sense, "New Space," which is usually presented as a sudden change of paradigm, shaking the foundations of a long-established and rigid industry, can rather be seen as a natural step in the evolution (maturation) of a budding sector. Notwithstanding, the rise of new actors and innovative ways of conducting space activities that is currently witnessed is undeniably opening new, sometimes unforeseen, prospects for the sector. These opportunities trigger, in turn, the emergence of new, and somewhat unexpected, challenges.

A top transverse issue in this new space era is, and will increasingly be, to continue ensuring the security, safety, sustainability, and stability (4S) of space activities and to safeguard our very capacity to deploy and operate systems in space. Indeed, space systems are exposed to an increasing level of "man-made" threats in addition to a naturally hazardous space environment (e.g., geomagnetic storms, solar radiations, etc.). This includes both unintentional hazards stemming from human activity (e.g., debris, interferences, etc.) and capacities to deliberately disrupt space systems or services (e.g., anti-satellite technologies, signal jamming, cyberattacks, etc.). Overall, an assessment of space security threats shows that they are (ESPI 2018):

- *Multiple and diverse* in nature and origin and, as a consequence, require a set of different mitigation and protection measures
- *Interrelated and interdependent* and therefore require a coherent and holistic approach adhered to by all space stakeholders
- *Ubiquitous and inclusive*, although some systems are less exposed or vulnerable to specific threats
- *Intensifying*, driven by endogenous and exogenous trends including a growing space activity, an increasing number of governmental and commercial actors, the emergence of new concepts, technologies and capabilities (e.g., mega-constellations, CubeSats, on-orbit services, etc.), an ever more connected and critical space infrastructure (i.e., making it a strategic target), or the rehabilitation of a "space warfare" doctrine encompassing activities to develop "space control" capabilities

As summarized in the US National Security Space Strategy in 2011, "space, a domain that no nation owns but on which all rely, is becoming increasingly congested, contested, and competitive" (U.S. Department of Defence 2011). This situation, expected to further deteriorate in the future, should be appraised in the context of a growing strategic and socioeconomic significance of space. As the use

of space applications becomes more pervasive, brings more benefits, and becomes part of the business-as-usual routine in many sectors, our dependence on space intensifies, which creates new vulnerabilities for the economy and society at large.

This deteriorating situation has already been widely acknowledged by European stakeholders including national governments, European institutions, and the private industry. The recognition of strategic interests in operating space systems in a secure, safe, and sustainable environment is now well integrated in key political documents. The Space Strategy for Europe clearly puts forward, “Europe’s autonomy in accessing and using space in a secure and safe environment” as a top priority European Commission 2016.

To date, the European approach to space security builds upon a multilayered structure of diverse frameworks and activities. Organized at national, intergovernmental, and European level, institutional efforts span across the spectrum of capacity-building programs, legal and regulatory measures, and diplomatic initiatives. Public undertakings are complemented by industry-led endeavors such as the Space Data Association which brings together satellite operators worldwide “to enhance safety of flight via sharing of operational data and promotion of best practices across the industry” (Space Data Association).

Despite multiple initiatives and noticeable achievements, European ambitions remain somewhat limited in comparison with other space-faring nations, especially the United States. In the field of Space Surveillance and Tracking (SST), for example, European resources for capacity building, from system development to service delivery, are 10–20 times lower than those available across the Atlantic for comparable activities. Here, differences in space budgets do not explain, alone, such a massive gap. Across the Atlantic, securing space assets has long been established as a strategic priority. The launch of a \$1.6 billion US Space Fence program aiming to further increase domestic Space Situational Awareness (SSA) capabilities and the recent publication of a National Space Traffic Management (STM) policy reminded the strong will of the US government to lead (or even rule) in this domain.

Along such recent developments, in the United States as well as on international scene, European policy-makers are realizing the criticality and urgency of setting up a more ambitious framework supported by adequate means commensurate to the level of challenges at stake. This already translated into an increase of the budget allocated by the EU to a European SSA program for the period 2021–2027 and into additional investments by France, among others, to support the development of national SST capabilities as part of a more ambitious *Stratégie Spatiale de Défense* adopted in July 2019 (Ministère des Armées 2019). Along these lines, more developments can be expected over the coming years including revised upward objectives and new support funds (i.e., European Defence Fund, Horizon Europe, ESA and national budgets, etc.).

While European resources for space security-related activities are likely to substantially increase over the next period, some structural issues may persist, in particular for what concerns coordination and leadership. Further progress in this direction is complex since it implies finding a new, suitable, and acceptable compromise on an appropriate balance between the need to preserve national sovereignty

over sensitive matters and ways to limit duplication of efforts under a TBD European leadership. Difficulties in this field are closely related to the overarching challenges of the European construction but also intimately linked to the multifaceted nature (individual/common, military/civil, institutional/commercial, etc.) which brings together various communities having different objectives and requirements to converge on joint solutions.

Nonetheless, stakes are high for Europe.

This chapter examines how the current European model successfully accommodated the interests of multiple stakeholders but may progressively reach some limits that could affect the place of Europe on the international scene. With a forward-looking approach, the chapter also discusses how some expected developments could impact the relevance and suitability of this model and shape its further evolution.

---

## Prospects for a European Space Security Policy

### Stakes Are High for Europe and Will Continue to Increase

The strategic significance of space security for Europe arises from its overarching ambition to “promote its position as a leader in space, increase its share on the world space markets, and seize the benefits and opportunities offered by space” (European Commission 2016). Achieving these objectives has a number of security-related implications.

In a recent study, the European Space Policy Institute suggested that public action in this domain is justified by four key rationales (ESPI 2018):

- *Secure the results of the continuous and substantial investment* made by public and private actors.
- *Protect the European economy and society* against risks related to its pervasive and sizeable dependence on the space infrastructure.
- *Contribute to a service-oriented policy* by assuring the ability of the infrastructure to deliver a service that can justifiably be trusted, in particular for users in defense and security.
- *Guarantee European autonomy and freedom of action* in the field of security in outer space and in the space domain at large.

### Socioeconomic Rationale and Service-Oriented Policy

Multiple studies and case studies demonstrated that space applications bring substantial socioeconomic benefits across numerous sectors (European Commission 2017). There is, however, a negative corollary to this: as the use of space-based solutions becomes more pervasive and part of business-as-usual, the dependence of governments, businesses, and consumers on space deepens, creating new risks. A study of the European

Commission estimated that an incapacitation of space systems – intentional or not – would lead to a significant economic loss of up to EUR 50 billion per year of gross added value and put up to 1 million jobs at risk in Europe (Ibid.). This is comparable, in size, to the entire European air transport sector. Furthermore, with the expected use of space capabilities (e.g., PNT signals, bandwidth, EO data) for new promising terrestrial technologies (e.g., autonomous vehicles, smart cities, precision agriculture), these risks will most likely increase in the future.

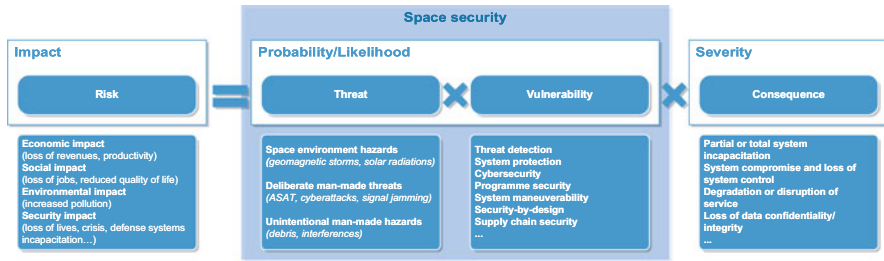
The criticality of mitigating the risks associated with a potential outage of space systems took a new meaning in Europe over the 2014–2020 period. With EU space infrastructure (i.e., Galileo, EGNOS, and Copernicus) fully operational and planning to complement these programs with a new initiative in the field of secure governmental communication (i.e., GOVSATCOM), the next Multiannual Financial Framework (MFF) (2021–2027) will give a high priority to exploitation, maintenance, and upgrade of space systems but also to the promotion of the services uptake in order to maximize the benefits of public investment in these programs. This entails the adoption of a service-oriented approach to build up user confidence through (1) a proven or certified level of performance, (2) the long-term availability of services, and (3) a service that can justifiably be trusted. This last condition translates into the need to take appropriate measures to protect the infrastructure against faults and threats. This requirement is a prerequisite for governmental and defense users that the EU seeks to support to reinforce and leverage synergies between civil and defense-oriented applications.

In short, the more Europe invests in and benefits from space, the more critical its responsibility to safeguard the space environment and infrastructure gets.

The socioeconomic rationale and service-oriented policy are already reasonable arguments for Europe to position security high in the space policy agenda. It can be legitimately expected that both of these drivers will further gain in prominence in the European space policy debate over the next Multiannual Financial Framework (MFF) period. As a means of illustration, the recent partial outage of the Galileo system brought to the front the sensitivity of space infrastructure security. Consequences of the outage were limited since – it must be stressed – the Galileo system is still under deployment. However, the event gave an early notion of the potential crisis that might have emerged in case of an unintentional, indelicate, or deliberate service disruption and underlined the importance of preventive measures to mitigate such risks.

## **European Autonomy and Weight on the International Scene**

Eventually, ensuring space security (i.e., mitigating risks associated with the exploitation of space systems) requires a variety of measures targeted to (1) mitigate threats to space systems on one hand and (2) reduce vulnerability of space systems on the other (see Fig. 1) (Note: Complementary measures targeting directly the source of the threats such as actions against cybercrime, space disarmament policies or radio spectrum management are not included here.):



**Fig. 1** Space security concepts and the relationship between them

As a consequence, it is clear that space security is a broad domain that encompasses many complementary areas and in particular:

- *Space Situational Awareness (SSA)*: Current and predictive knowledge and understanding of the outer space environment including space weather and location of natural and man-made objects in orbit around the Earth
- *Space Environment Protection and Preservation (SEPP)*: Preventive and curative mitigation of the negative effects of human activity in outer space on the safety and sustainability of the outer space environment
- *Space Infrastructure Security (SIS)*: Assurance of infrastructure ability to deliver a service that can justifiably be trusted despite a hazardous environment (i.e., security-by-design, security in operation)
- *Space Traffic Management (STM)*: Planning, coordination, and on-orbit synchronization of activities to enhance the safety, stability, and sustainability of operations in the space environment. (Note: As defined by the U.S. Space Policy Directive 3 on a National Space Traffic Management. Alternative, broader definition of STM exist such as the one from the IAA which describes STM as a wide encompassing concept (i.e. “the set of technical and regulatory provisions for promoting safe access into outer space, operations in outer space and return from outer space to Earth free from physical or radio-frequency damage”).)

Despite various past, current, and planned initiatives and measures across the board, Europe has not yet established a leadership in this field to express its concerns and represent its interests on the international scene and instead finds itself increasingly pressured by the proactivity of some other major players.

In the SSA domain, for example, a considerable share of European actors relies on data sharing agreements signed with the United States. This includes national ministries or armies (i.e., Belgium, Denmark, France, Germany, Italy, the Netherlands, Norway, Spain, the United Kingdom), European intergovernmental organizations (i.e., ESA, EUMETSAT), and commercial satellite operators and launch service providers. From a US perspective, SSA sharing agreements are powerful leadership instruments that aim to support transparency on operations in outer space, promote cooperation for security and safety, enhance the availability of

information among the partners, and improve the quality of US SSA information (Helms 2010; USSTRATCOM Public Affairs 2017). From a European perspective, they are now a critical input for SSA capabilities at large and, by extension, for the safe operation of space systems.

No need to remind here how much Europe greatly benefits from the open policy of the US government. The importance of transatlantic cooperation, in particular in defense and security domains, cannot be challenged. However, the gap between European and American capabilities, expected to increase with the deployment of the US Space Fence, creates a situation of reliance/dependence for European stakeholders and a major imbalance in cooperative arrangements. This state of affairs is in many respects beneficial for Europe but has also some strategic implications:

- *SSA data and service restrictions:* Although SSA data sharing agreements enhance the availability of information among the partners, restrictions exist. Because of its intrinsic military nature, a lack of transparency or a delay in information provision can occur for a variety of motives related to US national security. (Note: Specifically, the DoD resistance to open SSA data sets, algorithms, and processes to external review and scrutiny results in the uncertainty of the data and in possible false positive. See: <https://www.ida.org/idamedia/Corporate/Files/Publications/STPIPubs/2016/P-8038.ashx>.)
- *Reliability and accountability:* Although the most advanced worldwide, the US system is not flawless and may provide wrong information due to measurements or processing errors, in particular for smaller objects that Europe cannot track (Froeliger 2017). If European operators are blind, not being able to verify the data, they find themselves exposed to single points of failure.
- *Uncertainty on future access:* The US Government holds the right to terminate the agreement at any time for any reason, to limit both access duration and data amount, to deny access to SSA data and information, and to change or modify the terms and conditions at any time, and without prior notification (*Space-Track*).

From this perspective, although access to foreign SSA data and services is a relevant and effective way to augment domestic SSA capabilities, such access, even deemed unrestricted, free, and guaranteed, shall not sustainably remain a critical input on which they depend. For this reason and comparably to other fields such as access to space or critical technologies, Europe seeks to enhance its strategic autonomy in the SST/SSA domain, which is a pillar to establish any leadership in the space security domain. The objective to reach an “appropriate level of European autonomy” is addressed in most, if not all, policy documents setting the route for Europe in this matter. There is, however, no clear definition of a minimum, required, level of capabilities that would be strategically acceptable. Member States may also have different views on this question.

Overall, European stakeholders converge on the assessment that a fully effective approach to space security can only be envisioned as the outcome of a coherent and inclusive global effort and that cooperation with third countries, in particular the United States, is essential for many reasons. Autonomy is therefore not sought at

the expense of cooperation with key partners, but Europe shall ensure its capacity to control its level of reliance on third parties and to maintain it within acceptable boundaries.

Since space security will constitute an increasing and central share of the so-called space diplomacy, it can be reasonably argued that guaranteeing European autonomy and freedom of action in this field is a prerequisite to establish Europe's credibility and legitimacy in the global space arena. Europe's ambition to *promote its position as a leader in space* necessarily entails to play a central role (even as initiator) in international dialogues and negotiations as a promoter of a clear, united, and consistent "European way." From a more practical standpoint, to be positioned as a key player on the international space scene, Europe must contribute its share to this endeavor and ensure a balanced cooperation with other key players including, prominently, the United States.

## **Europe Is Mobilizing But Follows an Approach That Is Called to Evolve**

### **Space Security in Europe: A Multilayered Framework**

Space security is a complex issue because of the diversity of potential threats and mitigation or remediation measures that, in one way or another, impact all actors in space. As far as Europe is concerned, the multiplicity of stakeholders brings an additional layer of complexity.

In Europe, space security activities are primarily led and organized at national level, comparably to other security and defense domains:

- *National governments are the owners and operators of the main European SST systems.* These systems are operated in different ways according to the nature of ownership (civil/military) and to their purpose (scientific/operational). The diverse data they produce are also handled according to different protocols and data policy.
- *National space laws govern activities in space* by setting the requirements, conditions, and restrictions for licenses authorizing organizations to conduct launch and space operations. Some of these legal regimes contain provisions that actively contribute to space environment protection and preservation through obligations in the domain of space objects registration, space debris mitigation, or space systems reentry (Froehlich and Seffinga 2018).
- *National delegations hold voting rights in international diplomatic frameworks* such as the United Nations Committee on the Peaceful Uses of Outer Space (UN COPUOS) and the Conference on Disarmament (CD).

Despite a convergence of interests between different policy domains in the field of space security, the military and national security dimension remains prevalent at national level. (Note: The cross-domain aspect of space security is best illustrated by the United Kingdom's National Space Security Policy (2014), which resulted

from cooperation between the Ministry for Universities and Science, the Ministry for Defence Equipment, Support and Technology, the Ministry of State, and the Ministry for Immigration and Security.) Consequently, the most active countries in military space programs (i.e., France, Germany, Italy, the United Kingdom, Spain) are also the most active in space security. These countries may have different objectives, although overall convergent, that are set by national policy documents (space policy, defense policy). Different concerns and approaches gave rise to different governance models involving several ministries and organizations concerned by space security matters among which, of course, national space agencies. Efforts also remain uneven among the most proactive countries, in particular in the field of SST capacity building.

Although national sovereignty remains, so far, a structural component of space security in Europe, national action in this field has been flanked, since long, with the development of bi- and multilateral agreements for data sharing, resources pooling, operational coordination, or diplomatic collaboration among European countries. Dispositions to cooperate stem from a programmatic and geopolitical environment facilitating and promoting cooperation between European countries (i.e., European Union, ESA, etc.) but also from practical considerations concerning the capacity of each country to achieve, on its own, objectives requiring considerable resources. From this standpoint, national strategies underline a growing readiness and willingness to build on European cooperation in the field of space security. The involvement of European institutions in space security, namely, the European Union and the European Space Agency, obviously contributed to give raise to a new dimension in European cooperation. Building on bilateral and pan-European cooperation, the French *Stratégie Spatiale de Défense* declares in this respect that “beyond existing projects, a Europe of space must emerge to contribute directly to the construction of European security and defense on the continent. To do so the Franco-German motor must federate energies, in particular in the frame of a European SSA project” (Ministère des Armées 2019).

In this context, the role of the European Union in space security has grown within a broader and more political framework and at the crossroad between developments of the EU mandate and ambitions in the space domain on one hand and in the security and defense domain on the other. In this regard, the Lisbon Treaty (2009) was a stepping-stone for both domains, establishing shared competences between Member States and the European Union, but it is certainly the significant progress of EU space programs together with Jean-Claude Juncker’s Security Union ambitions that contributed more recently to make of the European Union an increasingly relevant actor in the space security field.

Notwithstanding a noticeable progress of its perimeter and involvement, the role of the Union in this field remains, so far, limited to support actions and diplomatic initiatives:

- *Support to R&D projects*, funded under the 7th and 8th Framework Programmes for Research and Technological Development (FP7, H2020) for a total contribution estimated around €68 million between 2007 and 2017. These projects cover a



wide range of different developments from SSA-related technologies to active debris removal solutions, including, among others, autonomous collision avoidance or space weather forecast.

- *Support to European SST cooperation*, with the establishment of a Space Surveillance and Tracking Support Framework in 2014 (European Commission 2014) to support the networking and operations of SST assets owned by EU countries and provide EU SST services with the EU Satellite Centre acting as front-desk and interface with users.
- *Diplomacy and international cooperation*, with the establishment of Space Policy Dialogues with key partners; active participation to international organizations and committees such as the International Telecommunication Union (ITU), the International Committee on Global Navigation Satellite Systems (ICG), or the UN COPUOS; the ill-fated proposal to establish an International Code of Conduct for Outer Space Activities; or the promotion of initiatives such as the Principles of Responsible Behavior for Outer Space (PORBOS) in the Conference on Disarmament.

The European Space Agency also plays an important role in the field of space security and safety, in particular for capacity building, R&D, and regulations/standards. Despite a convention that did not envision (but did not forbid either) activities in the field of space security and safety, ESA developed a recognized competence and expertise in the scientific and research dimension, with somewhat limited connection to national defense and security strategies. Eventually, the Agency “has evolved to conduct security related projects and programmes and to address the threats to its own activities” (Giannopapa et al. 2018). This evolution has been marked by the setting up of a comprehensive regulatory framework including ESA’s security agreement and security regulations and implementing procedures and facilities. ESA now has the capacity to receive, store, and produce classified information as well as to exchange classified information with third parties such as the EU Council, marking a step forward in the role that the Agency could play in the field of space security in the future.

Beyond security-related responsibilities in the management of space programs and the safe operation of its own space systems, activities of the Agency in the field of space security include noticeably:

- *An SSA program* funded by 19 ESA Member States through 2020 at approximately €200 million for the period 2009–2020 and dedicated to a variety of capacity-building projects including research and technology, set up and operation of data and coordination centers, and systems development and procurement across three main segments: Space Surveillance & Tracking, Space Weather and Near-Earth Objects.
- *The Clean Space Initiative*, which promotes an eco-friendly and sustainable approach to space activity throughout the entire life cycle of space systems from conceptual design to end of life and up to removal of debris with the

development of industrial materials, processes, technologies, and standards that are both Earth and space environment-friendly.

- *Participation to international fora* that work in different ways on space security including the International Astronautical Congress (IAC), the Committee on Space Research (COSPAR), the Inter-Agency Space Debris Coordination Committee (IADC), or the UN COPUOS of which ESA became an observer in 1972.

In addition to these central institutional actors and activities, the European space security landscape also encompasses other minor public activities as well as some private-led initiatives such as the participation of European operators to the Space Data Association, a non-profit association of satellite operators that supports the controlled, reliable, and efficient sharing of data that is critical to the safety and integrity of satellite operations.

---

## **Accommodating Different Concerns and Interests: Achievements and Limits**

As a result, the European framework for space security, which involves national and European (bilateral and multilateral) layers, civil and military organizations, public and private interests, and a broad range of concerns and needs, may seem intricate.

The overall European situation in the space security domain, including achievements and limits, is best illustrated by the SST/SSA component, which crystallizes many of the challenges ahead of Europe in this field.

Back in 2012, at the end of the Preparatory Phase of the ESA SSA program, several Member States decided to withdraw or reduce their contribution to the program component related to SST, with the objective of managing it through a different arrangement, more adequate to their needs. The main reason behind this decision was related to the prominence of military and operational functions in the SST domain and concerns about ESA capacity to properly manage security aspects, including compliance with defense requirements and handling of classified information and data. Some Member States, especially France and Germany, also raised some concerns related to national sovereignty. German and French military organizations negotiated and prepared a non-paper submitted to the European Commission in December 2012 which requested the establishment of a new mechanism at EU level with a specific governance scheme where Member States could maintain control over their assets while cooperating in SST activities. The objective was then to promote a framework that would foster pan-European cooperation and improve cost efficiency (e.g., by avoiding unnecessary duplication of efforts) to deliver EU SST services while complying with national concerns resulting from the specific nature of SST systems and data. In compliance with the principle of shared competences between the European Union and Member States in the field of security

and space, the framework would also enable to transfer a share of the financial burden to the European Union. Eventually, the Space Working Party in Brussels started to negotiate the contents of what became Decision No 541/2014/EU of the European Parliament and of the Council of 16 April 2014 establishing a Framework for Space Surveillance and Tracking Support (European Commission 2014).

The outcome of this framework are, at this stage, mixed. The framework has been instrumental to reinforce European coordination (i.e., complex systems networking, delivery of European services, common database of unclassified data, enhanced bilateral agreements for classified data, etc.) and to build confidence among partners but does not seem to provide, in its current form, the best configuration to avoid duplication of efforts and support an efficient development of EU SST capabilities, necessary to close the capability gap and achieve an acceptable level of European autonomy while meeting the needs of a variety of users throughout the entire space mission life cycle (European Commission 2018).

To put things into perspective, it is important to remind that the current arrangement allowed, first and foremost, to accommodate the requirements, sometimes divergent, of different parties. In essence, the intergovernmental model is meant to mitigate two conflicting objectives:

- *Leverage cooperation* among the most motivated Member States to share efforts and results between partners to enhance efficiency and performance of European capabilities
- *Preserve national interests* by safeguarding national sovereignty over dual capabilities development and control over SST systems and data

Beyond issues related to the level of resources available to support European objectives in space security, many blocking points arise from the unresolved question of the relative weight of national interests and European cooperation and therefore of the sharing of responsibilities between Member States and with the EU. For example, the role of the European Commission is rather limited in the current configuration, even though it is the principal funding source and holds the responsibility over the security of the EU space program. From a very practical perspective, two immediate risks come to mind:

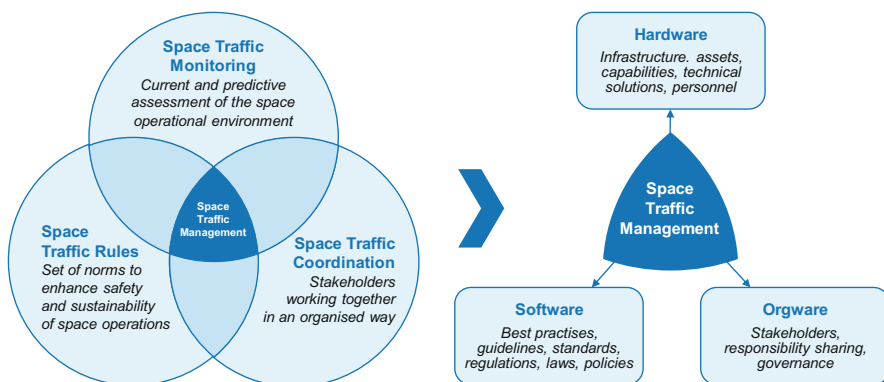
- *A risk of divergence of interests among stakeholders* (between Member States and with the European Union), hindering the capacity to implement a coordinated policy. This risk is growing as stakeholders' concerns and positions on space security issues tend to progress faster than European integration and leadership.
- *A risk of duplication of efforts and reduced cost-effectiveness*, if motives to develop specific national capabilities surpass the willingness (and readiness) to focus on distribution and complementarity across Europe. This risk is also growing as the need to optimize resource utilization increases with the overall cost of required capabilities to provide necessary coverage and precision.

An important step forward is the preparation of the next Multiannual Financial Framework 2021–2027 of the European Union. Yet, although an increased level of financial resources can be expected to support SST/SSA (from multiple sources), the current version of the regulation (still to be officially endorsed) proposes mostly to maintain the current model with an enlargement of contributing Member States. With the objective to develop the performance and autonomy of capabilities, the SST component of the EU space program should still build on a network of mostly national SST sensors and support operation and delivery of SST services. The principles of complementarity and the necessity to avoid duplication are recalled but not formally enforced since room is left to develop redundant capabilities.

### Space Traffic Management: A Coordination and Leadership Challenge

The limits of the current approach to space security, in particular those related to European coordination and leadership, have recently been accentuated by the announcements of the US government regarding space traffic management which invite other space-faring nations, and in particular Europe, to take position in this domain as well.

With the recent adoption of a National Space Traffic Management Policy, the United States made a major step forward in recognizing the severity of issues at stake and the urgency of setting up a framework to address space security challenges, in particular those related to the expected boom/change in space traffic (deployment of mega-constellations, non-maneuverable CubeSats, in-orbit services, etc.). In this context, the US policy aims to “develop a new approach to space traffic management that addresses current and future operational risks” (White House 2018). Such approach necessarily encompasses a wide range of measures for the development of space traffic monitoring capabilities, the requirements related to space traffic rules, and the coordination of various stakeholders (see Fig. 2).



**Fig. 2** Representation of space traffic management components

Although national, the policy does not inherently challenge the relevance of multilateral efforts in this field and actually recalls that “it is a shared interest and responsibility of all spacefaring nations to create the conditions for a safe, stable, and operationally sustainable space environment” (Ibid.). However, it opens the door to the development of multiple, possibly divergent, national and regional STM frameworks in parallel to international discussions. It also sets the intention of the US government to take leadership in this field through different means including enabling greater SSA data sharing, developing and promoting space safety standards and best practices across the international community, and encouraging and facilitating US commercial leadership.

The rising need to address new safety and sustainability challenges associated with the development of space activities and the US determination in this domain should create a strong impetus for Europe to take up the issue now and move forward with the definition and implementation of its own policy for space traffic management. It is also a matter of protecting Europe’s industrial and commercial interests to set adequate standards and norms for future STM services markets as well as means to foster Europe’s credibility on the international scene.

Setting up an effective STM framework is a serious challenge, and even though the US directive sets the principles, goals, roles and responsibilities, as well as guidelines to be followed, the concrete implementation of such policy proves to raise major difficulties. Much of the issues faced across the Atlantic have to do with the transverse challenge of bringing together the views and capabilities of multiple stakeholders (See: [Hitchens](#), See also: [Weeden](#)). Greater coordination, harmonization, and convergence between actors are at the heart of the various STM components:

- *To enhance SSA data* and reach the appropriate level of coverage and precision to safely manage operations in orbit, STM involves a better pooling and sharing (or purchasing) of data and services. This implies the necessity to address collective information management (collection, fusion, distribution) to safeguard data quality, availability, integrity, and confidentiality. It also implies more transparency from operators.
- *To specify and promote safety and sustainability norms*, STM involves the definition of best practices, technical guidelines, safety standards, or regulations addressing the full life cycle of space systems and applicable (possibly tailored) to a wide range of actors. This implies to make the interests of different actors converge in a balanced framework. It also implies some kind of arbitration between conflicting views.
- *To distribute roles and responsibilities*, STM involves to clearly delineate domains of activity (military/civil, public/private, national/international) and to establish the appropriate channels between them. This is essential to simultaneously achieve national security, commercial, and diplomatic objectives.

Comparable coordination challenges will arise in Europe as well. Given the state of affairs previously described, the lack of top-down leadership and the national/regional dimension will likely bring an additional layer of complexity.

---

## Conclusions

As Europe is contemplating its next 7-year period, some forward-looking reflection seems in order. Incidentally, the projections are clear: if the space sector continues to mature and develop along anticipated trends, coming years will be marked by a steep increase in space traffic, a diversification of actors, the emergence of new concepts, possibly rising tensions, and, in general, a serious degradation of safety conditions in space putting at risk the sustainability of in-orbit operations in the long term. In front of these challenges, a proportionate response is necessary if Europe wants space to continue to serve as a strong socioeconomic engine but also if it intends to engage in a more assertive approach to security and defense and to hold its place around the table of negotiation of international space affairs.

European stakeholders share, today, the awareness of the growing urgency and criticality of issues at stake. They also certainly share the conviction that a successful response to space security challenges should be articulated around a comprehensive and coherent approach building on an appropriate level of resources and on European cooperation in view of a global solution. This ideal approach will, as usual, need to be confronted to the complexity inherent to the conduct of European affairs. However, the fast pace of evolution of the situation, both in orbit and on the ground, presses for decisions to be made in the short term.

In this respect, the European approach to space security shall be objective driven, rather than dictated by pre-existing processes and institutional constraints. Given the wide-encompassing range of safety and sustainability issues at stake, the definition of a European Space Traffic Management regulation and operational setup, as a first step toward a full-fledged European space security policy, probably requires dedicated and innovative decision-making processes. This a matter of complementing the current bottom-up approach building on operational collaboration with a top-down leadership, empowered to define principles, goals, roles and responsibilities, as well as guidelines to be followed in Europe.

While the current European setup – designed to accommodate the interests of various stakeholders – allowed to progress substantially on many technical and cooperation challenges, questions arise on its capacity, in its current form, to tackle the emerging challenges that will continue to intensify over the next 7 years and beyond. In light of the rising stakes and challenges for Europe in the field of space security, moving from an “accommodation” to a “convergence” of interests – while preserving core national sovereignty concerns – seems to be an increasingly pressing issue. To this end, further progress shall be made in terms of balancing national interests against the merits of a European cooperation and therefore in terms of sharing of responsibilities among Member States and with the EU.

Such progress cannot be isolated from the broader foreign and security political context. While space has long been nested in European cooperation, it is not the case of the foreign and security policy, which has been, for the largest part and so far, left aside of the EU framework. We are observing at the moment the premises of a movement in this direction, which will have profound political and cultural implications at European level, as well as on the global scene.

In this context, space security might actually serve as an adequate test case for the European Union and its Member States (in collaboration with relevant organizations such as ESA) to experiment new forms of arrangements giving more room to European leadership and cooperation to serve shared interests:

- Space security is a comprehensive issue that involves a wide range of key concerns (i.e., programmatic, financial, regulatory, diplomatic, etc.) that make it a good candidate to be considered not only as a transverse matter but also as a possible full-fledged programmatic and policy domain.
- Space security is inherently a dual topic offering promising perspectives of synergy between space and defense. At the crossroad of military and civil domains with already existing interactions, it also involves competitiveness and innovation challenges and opportunities for the European industry.
- Space security already has strong European cooperation foundations, and various structures – meant to evolve along with policy objectives – are in place, including for SST capabilities development or for the security component of programs of direct military significance such as Galileo. For these different structures, there is a strong European added-value, both to deliver operational services and optimize cost-effectiveness.
- Space security will likely be subject to profound changes in the next few years, expected to ease up some of the current difficulties in this matter. For example, several experts anticipate a trend toward more transparency between space players, including military ones. In this respect the development of new capabilities, commercial in particular, may lead to a paradigm shift in the value of data confidentiality versus availability. Another interesting trend is the growing readiness of many public and private stakeholders to consider more stringent regulations.

Last but not the least, space security involves a strong link between internal and external action. That could make it an excellent candidate to support a more strategic, more assertive, and more united Europe in the World, as the incoming President-elect of the European Commission, Ursula von der Leyen, called for in her mission letter to Josep Borrell, High Representative of the Union for Foreign Affairs and Security Policy (von der Leyen 2019).

---

## References

- ESPI. Security in outer space: rising stakes for Europe – report 64, August 2018
- European Commission (2014) Decision no 541/2014/EU of the European Parliament and of the council of 16 April 2014 establishing a framework for space surveillance and tracking support

- European Commission. Communication from the Commission to the European Parliament, The Council, The European Economic and Social Committee and the Committee of The Regions. Space Strategy for Europe. COM (2016) 705 final, October 2016
- European Commission, Dependence of the European economy on space infrastructures: potential impacts of space assets loss, March 2017
- European Commission (2018) Report from the commission to the European Parliament and the council on the implementation of the space surveillance and tracking (SST) support framework (2014–2017)
- Froehlich A, Seffinga V (2018) National space legislation. European Space Policy Institute (ESPI)/ Springer, Vienna
- Froeliger JL (2017) Greater industry cooperation needed to avoid space collisions. INTELSAT. Retrieved from: <http://www.intelsat.com/news/blog/greater-industry-cooperation-needed-to-avoid-space-collisions/>
- Giannopapa C, Adriaensen M, Antoni N, Schrogl K-U (2018) Elements of ESA's policy on space and security. *Acta Astronaut* 147(2018):346–349
- Helms S. Space situational awareness. Power point presentation for the United Nations Committee on Peaceful Uses of Outer Space (COPUOS), June 3, 2010
- Hitchens T. #SpaceWatchGL Op'ed: New space debris rules stalled by year-long interagency spat. Retrieved from <https://spacewatch.global/2019/09/spacewatchgl-oped-new-space-debris-rules-stalled-by-year-long-interagency-spat/>
- Ministère des Armées, Stratégie Spatiale de Défense, July 2019
- Space Data Association website. <http://www.space-data.org/sda/>
- Space-Track. User agreement. Retrieved from [https://www.space-track.org/documentation#/user\\_agree](https://www.space-track.org/documentation#/user_agree)
- U.S. Department of Defence. National Security Space Strategy, January 2011
- USSTRATCOM Public Affairs (2017) U.S. strategic command, Norway sign agreement to share space services, data. Retrieved from U.S. Strategic Command Peace is our Profession Retrieved from <http://www.stratcom.mil/Media/News/News-Article-View/Article/1142970/us-strategic-command-norway-sign-agreement-to-share-space-services-data/>
- von der Leyen U. Mission letter to Josep Borrell, High representative of the Union for Foreign Policy and Security Policy/Vice-President designate of the European Commission, 10 September 2019, Brussels
- Weeden B. Time for a compromise on space traffic management. Retrieved from <http://www.thespacereview.com/article/3673/1>
- White House (2018) Space policy directive-3, National Space Traffic Management Policy





# Space and Security Policy in Selected European Countries

# 25

Ntorina Antoni, Maarten Adriaensen, and Christina Giannopapa

## Contents

Introduction .....	468
National Space and Security/Defense Strategies .....	469
France .....	473
Germany .....	475
Italy .....	476
Spain .....	478
The United Kingdom .....	479
Priorities and Trends in National Space and Security/Defense Strategies .....	481
Conclusion .....	482
References .....	482

## Abstract

This chapter presents space and security policies of selected European countries and indicates the main priorities and trends thereof. In particular, it addresses relevant strategic documents that show how certain states in Europe use space assets and applications to ensure security policy objectives. Recent developments at the national level are linked with space policymaking in the frame of the European Union and the European Space Agency.

---

N. Antoni (✉)  
Eindhoven University of Technology, Eindhoven, The Netherlands  
e-mail: [ntorina.antoni@gmail.com](mailto:ntorina.antoni@gmail.com)

M. Adriaensen · C. Giannopapa  
European Space Agency (ESA), Paris, France  
e-mail: [maarten.cm.adriaensen@gmail.com](mailto:maarten.cm.adriaensen@gmail.com); [christina.giannopapa@esa.int](mailto:christina.giannopapa@esa.int)

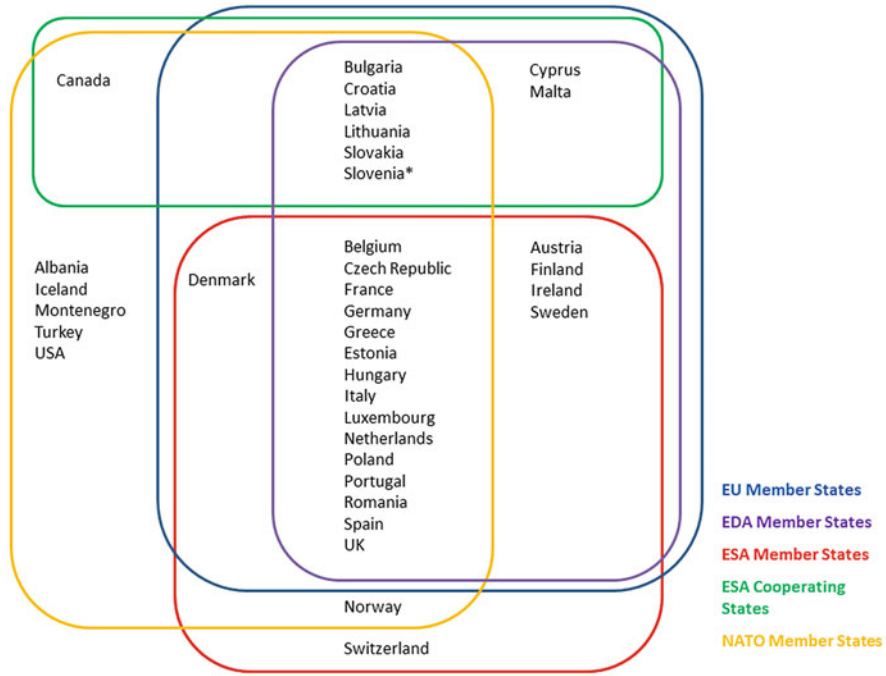
## Introduction

Europe is a continent consisting of a multitude of national, intergovernmental, and supranational organizations with diverse space policy priorities, thereby creating a multifaceted and dynamic space sector. By and large, the European space sector has been interwoven with the European integration process, which has been central in addressing rising security challenges including climate change, migration, and cybersecurity. Space policies have contributed to reinforcing European cooperation and integration in order to tackle these challenges. In addition, the surge in the number of private commercial actors as well as the emergence of a civil-military paradigm has resulted in the transformation of the space sector. The advent of a new era in space in combination with particular dynamics in the European space sector has put space security at the forefront of policy and regulatory debates.

The main actors in Europe engaging in space and security activities are the European countries, the European Union (EU), and the European Space Agency (ESA). The EU Global Strategy, adopted by the European Council in June 2016, the European Commission Space Strategy for Europe, launched in October 2016, and the European Defence Action Plan 2016 all stress the importance of space security. More recently, in June 2018, the EU presented the Proposal for a Regulation for a Space Programme for the EU (European Commission 2018). Furthermore, ESA has increasingly contributed to space security “in” and “from” space, as reflected in the Council Document “Elements of ESA’s Policy on Space and Security,” issued in June 2017 (Giannopapa et al. 2018). In December 2019, the Council at the Ministerial level adopted the “safety and security pillar” along with associated programs. With regard to ESA–EU relations, in October 2016, they signed the Joint Statement on Shared Visions and Goals, while in May 2019 they convened the first joint Space Council in 8 years (Spacewatch.global 2019). It is also worth mentioning that the North Atlantic Treaty Organization (NATO) has increased its interest in the use of space assets for defense, with the most notable milestone being the adoption of space policy in June 2019 (Euractive 2019). For further information about the institutional and various space and security programs in Europe, please see the respective chapters in this Handbook.

The different space security policies of the European countries are to a large extent determined by national needs and priorities as well as their participation in relevant space and security organizations. Figure 1 below visualizes the current status of the countries’ membership to ESA, EU, EDA, and NATO (adapted from Papadimitriou et al. 2019). In the present chapter, the European countries with the largest ESA annual budget and their defense expenditure as share of their gross domestic product (GDP) are presented. Namely, these are: France, Germany, Italy, Spain, and the United Kingdom (UK).

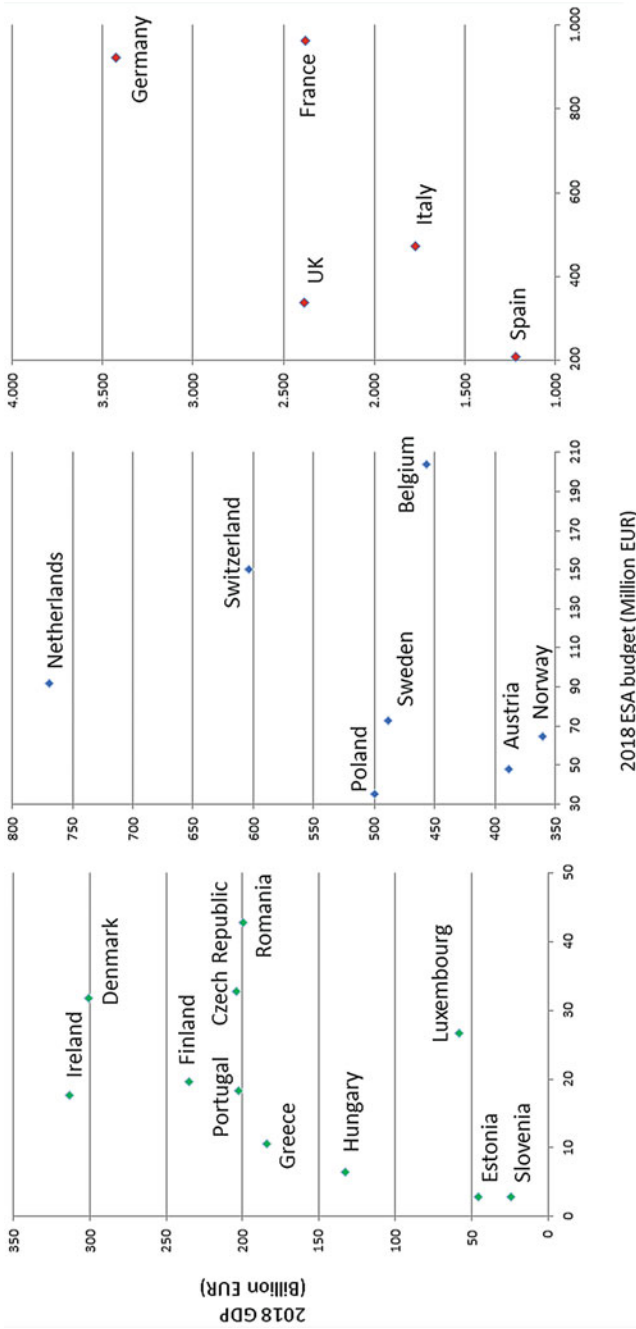
The aforementioned countries may be distinguished not only on the basis of their membership to these organizations but also based on their space budget. In the absence of an official grouping of these countries within any of the aforementioned organizations, their ESA annual budget and their defense expenditure as share of their GDP are used in this chapter to classify them into three groups, as seen in Figs. 2 and 3.



**Fig. 1** EU, ESA, EDA, and NATO Member States (Papadimitriou et al. 2019) (\*Slovenia is an ESA Associate Member State)

## National Space and Security/Defense Strategies

The current priorities and trends in national space and security strategies of the mentioned European countries derive from space and security elements stipulated in strategic documents. All countries included in this study have established their strategic priorities in the field of space and security mainly in the following types of documents: National Defense Strategy and Doctrine, National Defense Procurement Strategy and Policy, National External or Internal Security Strategy, and National Space Strategy or Policy. Depending on the country, more specific documents complement the strategic landscape, for instance, through a dedicated space security strategy or through the inclusion of space and security aspects in strategy documents covering other policy areas. For example, space and security aspects can be found in maritime strategies and arctic strategies that also stress the importance of space-based assets and applications in these domains. An overview of space and security strategic documents, which have been studied to analyze the priorities and trends in the European countries with the largest space and security budget – France, Germany, Italy, Spain, and the United Kingdom – is presented in Table 1.



**Fig. 2** ESA Member States 2018 GDP versus 2018 ESA space budgets categorization in three groups (ESA and IMF World Economic Outlook)

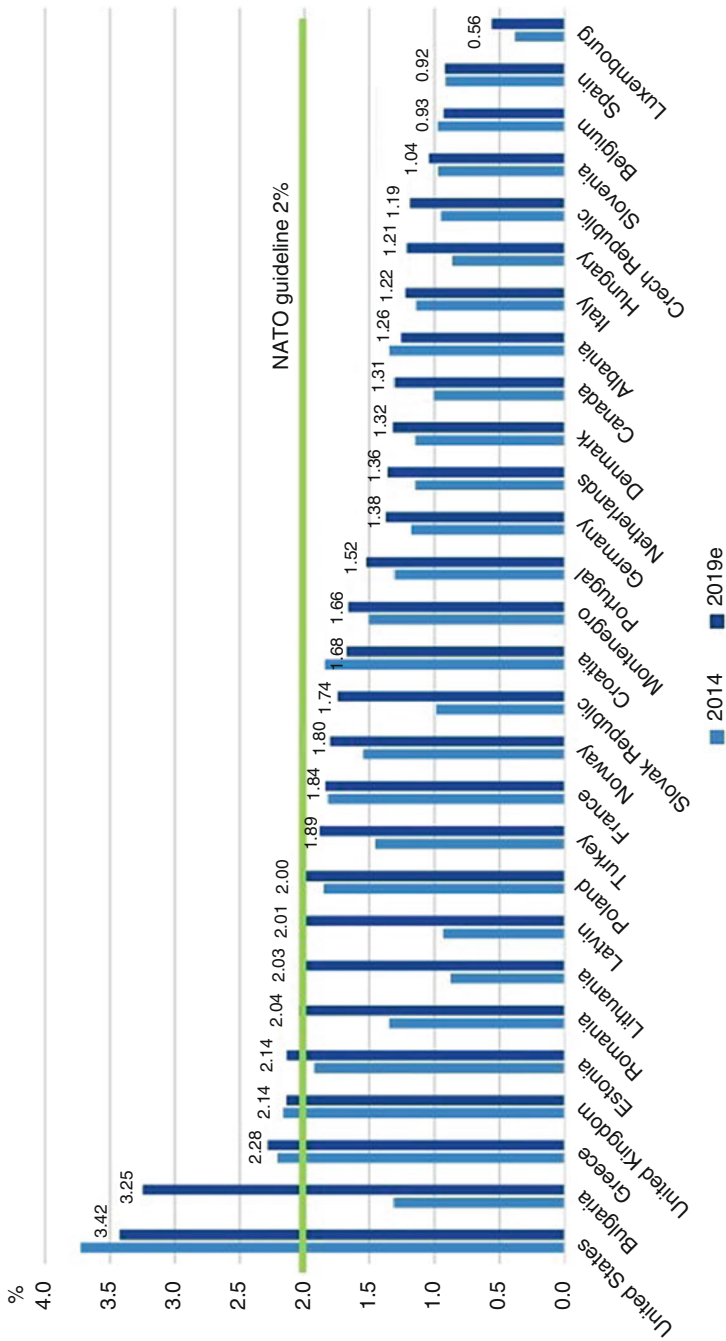


Fig. 3 NATO defense expenditure as share of GDP (%) (NATO 2019)

**Table 1** Strategic documents on space and security for selected European countries

	National Space Law	National Space Strategy/Policy	National Security and Defence Strategy/Policy (other relevant domains)
France	2008 Law concerning Space Operations (French Space Operations Act)	2019 Space Defence Strategy 2015 Ambition 2020–2015, Space for the climate 2012 French Space Strategy	2017 Defence and National Security Strategic Review 2015 French National Strategy for the security of maritime areas 2013 French White Paper on Defence And National Security and Bill on Military Planning 2014–2019 (updated 2019–2025)
Germany	2007 Satellite Data Security Act 1990 Law Governing the Transfer of Responsibilities for Space Activities	2010 making Germany's space sector fit for the future – the space strategy of the German Federal Government	2018 High-Tech Strategy 2025 2016 White Paper on German Security Policy and the future of the Bundeswehr
Italy	2018 Space Bill containing measures for the coordination of the space and aerospace policies along with important regulations concerning the organization and functioning of the Italian Space Agency-ASI	2019 Government guidelines on space and aerospace 2016 Strategic Vision Document 2016–2025	2019 National Security Strategy for Space 2018 Pluriennial programmatic document 2015 White Paper for International Security and Defence
Spain	1995 Royal Decree 278/1995 establishing in the Kingdom of Spain the Registry foreseen in the Convention adopted by the United Nations General Assembly on 2 November 1974	Spanish Strategy for ESA and EU Space Programs 2007–2011	2017 IDS (infodefensa) R&D strategic approach 2013 National Security Strategy – sharing a common project 2012 National Defence Directive 1/2012
United Kingdom	1986 Outer Space Act	Defence Space Strategy (under development) 2015 National Space Policy 2015 Space Innovation and Growth Strategy 2014–2030 2014 National Space Security Policy 2013 Strategy for Earth Observation from Space (2013–2016) 2012 UK Civil Space Strategy	2015 National Security Strategy and Strategic Defence and Security Review

## France

### Space and Security Status

France is a permanent member of the United Nations (UN) Security Council. France has been at the forefront of the elaboration of the EU Common Security and Defense Policy (CSDP). France is a member of the G7 and G20. France was one of the founding members of the NATO in 1949. France is a member of EDA and the European Union Satellite Centre (SatCen). France is a member of the Organisation for Joint Armament Cooperation (OCCAR). France has established and maintained extensive bilateral relations with European partners on security and defense, notably with Germany, Italy, and the UK. France was one of the founding member states of ESA in 1975. Also, Paris hosts the ESA Headquarters. Created in 1961, under the joint supervision of the Ministry of Higher Education, Research and Innovation and the Ministry of the Armed Forces, the National Centre for Space Studies (CNES) is the national space agency, a public administration institution with industrial and commercial purpose (*établissement public à caractère industriel et commercial*), charged with developing and executing the French space program. CNES prepares the French space policy under the responsibility of the Minister for Higher Education, Research, and Innovation, while it has a partnership with the Ministry of Defense for military space activities.

### Space and Security Elements in Strategic Documents

Space operations in France are regulated by the 2008 Law concerning space operations, the “French Space Operations Act” – *Loi sur les Opérations Spatiales*. The French Space Operations Act sets up a national regime to authorize and control space operations based on international commitments of the French government. The Act sets out an authorization regime with specific conditions, procedures, and technical requirements along with a control regime and mechanism (French Republic 2008). The Act lays down safety and security standards for the Guyana Space Centre and defines the liability regime for space activities. The 2012 French Space Strategy published by the Ministry of Research establishes a directorate of innovation, applications, and science to support new space. It also identifies security and defense as one of the specific applications and orientation areas for the French space policy (French Republic 2012). In particular, the development axes of the 2012 Space Strategy include very high resolution (VHR), secure satellite communications (SATCOM), electronic intelligence (ELINT), and detection and early warning for ballistic missiles. Defense aims to fully benefit from the dual-use nature of space systems (French Republic 2012). On top of that, the CNES ambition 2015 stresses the relevance of VHR optical observation, electronic intelligence, ultra-secure telecommunications, and space situational awareness (SSA) for defense purposes (CNES 2015).

In terms of security and defense, the French 2017 Defense and National Security Strategic Review emphasizes “the need to develop space situational awareness and to ensure the resilience of space capabilities.” It also refers to space as “a provider of essential navigation, communication, meteorological and imagery services, while

also a domain of confrontation where some states can be tempted to use force to deny access or threaten to damage orbiting systems.” The list of operational capabilities, required for a coherent and full-spectrum model, includes imagery intelligence (IMINT), Electronic Intelligence (ELINT), Command and Control (C2), and the protection and security of space assets requiring adequate SSA. It stipulates that “space is of crucial importance to defense capabilities, while becoming an increasing source of vulnerability for C2 and surveillance assets. Monitoring objects in low earth orbits – and watching geostationary orbits, as planned for by the aerospace operations command and control system (AOCCS) – is essential to ensuring the security of our space-based assets and conducting operations [. . .] An early warning capability would enable better characterization of ballistic threats, determination of the source of a launch and prediction of the target area.” The strategic review further stresses the relevance of enhancing satellite-based surveillance for maritime security (French Ministry of the Armed Forces 2017).

Moreover, the 2013 French White Paper on Defence and National Security and the Bill on Military Planning 2014–2019 (updated 2019–2025) highlight the strategic function of space-based systems: “Outer space has become crucial to the operation of essential services (French Ministry of the Armed Forces 2013). In the military field, strategic autonomy is dependent on free access to and use of space, which make it possible to preserve and develop the technological capabilities on which the quality of our defense system and, not least, the credibility of our nuclear deterrent, depend.” The White Paper refers to increasing threats from space debris promulgation and offensive space weaponry. The Bill foresees the delivery of three *Composante Spatiale Optique* (CSO) satellites no later than 2021 and plans the launch of a third Syracuse satellite by 2030.

Space, security, and defense policies in France are merged under the recently released 2019 Space Defence Strategy that intends to respond to challenges from the emergence of New Space (French Ministry for the Armed Forces 2019). As stated, “this new environment implies a Space Defence Strategy founded on the protection of French capabilities. That involves first and foremost improving Space Situational Awareness (SSA), especially in order to detect and attribute unfriendly or hostile acts in all orbits of interest and defend against them.” In order to guarantee France’s capacity to act in space, the armed forces aim to “(i) strengthen a space doctrine which establishes the ground rules for and typology of military space operations, (ii) overhaul military space governance, and (iii) ensure that they have appropriate capabilities and human resources.” Accordingly, “military space operations consist in operating space capabilities that provide services in support of government authorities and military operations, thus helping to increase the effectiveness of action. They contribute to national security, the robustness of economy and protection of the population. They also include action taken in space to protect assets and discourage any aggression. They are organized around four functions: space service support; space situational awareness; operations support; and active space defense” (French Ministry for the Armed Forces 2019). The 2019 Space Defense Strategy is aligned with the previously published security/defense and space strategy documents.



Last but not the least, in the maritime domain, the 2015 French National Strategy for the Security of Maritime Areas addresses the relevance of space-based resources for the monitoring of French maritime areas, including Satellite – Automatic Identification System (SAT-AIS), long range tracking and identification (LRIT), vessel monitoring systems (VMS), and Earth observation imagery (French Republic 2015). In that regard, France considers requirements for satellite surveillance in maritime areas. The strategy highlights the weaknesses in resilience and security of SAT-AIS. The strategy refers to the role of industry in providing solutions for the governments' requirements for maritime surveillance including radar or optical satellite imaging, spatial AIS, and satellite communications.

## Germany

### Space and Security Status

Germany is not a permanent member of the UN Security Council. Germany is a member of the G7 and G20. Germany was one of the founding members of the NATO in 1949. Germany is a member of EDA and SatCen. Germany is a member of the OCCAR. Germany and France have a strong history of cooperation in defense. Germany also works closely with the Netherlands in the defense realm. Germany was one of the founding member states of the ESA in 1975. The German Ministry for Economic Affairs and Energy (*Bundesministeriums für Wirtschaft und Energie – BMWi*) is mainly responsible for Germany's civilian space activities.

### Space and Security Elements in Strategic Documents

Space activities are governed by the Law of 8 June 1990 Governing the Transfer of Responsibilities for Space Activities (*Raumfahrtaufgaben Übertragungsgesetz*) and the 23 November 2007 Satellite Data Security Act (German Federal Ministry of Justice 1990, 2007). The Law delegates the responsibility for the management of the German space program from to DLR (German Aerospace Center – *Deutsches Zentrum für Luft- und Raumfahrt*).

The 2010 German Space Strategy addresses space security based on the approach of “whole-of government security preparedness,” which includes not only space-based early warning for impending crises but also increased sensitivity for the importance of an unhindered use of satellite systems for national security (BMW 2010). Accordingly, “Satellite data and services make a vital contribution, notably to disaster relief and management, environmental and climate protection, to warning of threats, development aid, border monitoring, and arms control. In this regard, it is stated that:

- “Military operations are now inconceivable without the support of space-based systems;
- Space systems in the domains of communication, navigation and Earth observation make a decisive contribution to the ability to conduct an effective foreign and security policy and to achieve whole-of-government security preparedness;

- Wherever possible, exploit synergies between civil developments and dual-use technologies when further developing system capabilities and strategically important competences in key technologies” (BMW 2010).

In the context of security and defense, the 2016 White Paper on Security Policy and the Future of the *Bundeswehr* notes that satellite systems are a fundamental component of Germany’s critical infrastructure. All aspects of national and international communication and navigation decisively depend on them. The White Paper thus stresses the need for monitoring these critical systems. In line with the EDA Capability Development Plan (CDP), Germany’s common security priorities in the White Paper include UAVs, air-to-air refueling, satellite communication, cyber protection, and cyber defense (German Federal Government 2016). The 2015 Joint Concept for Space, commissioned by the Ministry of Defense, acknowledges that space is an operational domain of its own. Space support to operations has become an indispensable military function and as such, it requires the establishment of situational awareness and of the necessary command and control functions for the space domain (Japan Space Forum 2015).

What’s more, the White Paper on German Security Policy and the Future of the *Bundeswehr* from 2006 highlights the capability category of intelligence collection and reconnaissance and the procurement of the SAR(Synthetic Aperture Radar) LUPE space-based reconnaissance system. Using a joint approach: efficient command, control, and information systems of the armed forces ensures the capability to exercise command and control worldwide. The White Paper describes joint that networkable radio equipment and “SATCOMBw,” satellite-based communications system, are important prerequisites for network-enabled operations (German Federal Government 2016).

Finally, the 2025 high-tech strategy emphasizes using the potential of key technologies for the benefit of the industry including space technologies (German Federal Government 2018). In particular, “to ensure technological sovereignty in the area of satellite infrastructure,” the strategy elaborates on the establishment of the Institute for Satellite Geodesy and Inertial Sensors of DLR in Hanover and Bremen, the DLR Institute for Quantum Technologies in Ulm, and the DLR Galileo Competence Center in Oberpfaffenhofen. The most important objective is to support industry in the transfer of research results from the field of quantum technology and artificial intelligence into practical application including the aerospace sector (German Federal Government 2018).

## Italy

### Space and Security Status

Italy is not a permanent member of the UN Security Council. Italy is a member of the G7 and G20 and was one of the founding members of the NATO in 1949. Italy is a member of EDA and SatCen, as well as OCCAR. At the bilateral level, Italy and France have active collaboration on space, reflected in annual summits organized

since 1982. Italy was one of the founding member states of ESA in 1975. In Italy, responsibility for space activities has recently been put directly under the supervision of the Prime Minister.

### **Space and Security Elements in Strategic Documents**

The Italian Parliament approved on 22 December 2017 the new 2018 Space Bill containing measures for the coordination of the space and aerospace policies along with important regulations concerning the organization and functioning of the Italian Space Agency – ASI. ASI reports directly to the Prime Minister’s Office. The Bill mainly provides that the management and coordination of space and aerospace policies are assigned to the Presidency of the Council. The Bill also established an inter-ministerial Committee that will be responsible for defining the government’s orientations in the sector (Italian Parliament 2018).

In July 2019, the National Security Strategy for Space was presented to promote a “systemic” strategy for national security (Italian Presidency of the Council of Ministers 2019). The strategy was based on the March 2019 Government guidelines on space and aerospace (Italian Prime Minister’s Office 2019). The strategic objectives of the National Security Strategy for Space are: (a) “to ensure the security of space infrastructures (according to the two Anglo-Saxon terms, safety and security), regarded as enablers of the national infrastructure as a whole; (b) to safeguard national security, including through space, by ensuring access to and use of national security capabilities in any given situation; (c) to strengthen and protect the institutional, industrial and scientific sectors, also with a view to protecting national classified information; (d) to promote a space governance capable of ensuring sustainable, safe and secure space operations at international level; (e) to ensure that the development of private initiatives in the space sector (upstream and downstream) is consistent with the country’s overriding interests” (Italian Presidency of the Council of Ministers 2019).

According to the Strategy, *safety* is defined as “a set of measures put in place to ensure protection against unintentional events,” while *security* is defined as “a set of measures to guarantee security against malicious activities or actions carried out by opposing parties.”

Additionally, the ASI Strategic Vision Document 2016–2025 highlights the use of space assets also for security and defense purposes (ASI 2016): “Earth observation data for needs of crisis management, security, defense, and disaster monitoring:

- Space Situational Awareness (SSA), Space Traffic Management, Confidence building measures, Code of Conduct;
- Promotion of institutional services: climate, environment, managing the cycle of risks and emergencies, weather-sea and atmosphere monitoring, national security with maritime surveillance, border control and humanitarian aid;
- Development of domestic GNSS activities, Public Regulated Service (PRS) security center, interference monitoring center, PRS terminals, interfaces and networks for domestic users; Ensure Italy’s role and participation in the processes of multilateral international coordination in various international contexts of a

global nature, like the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) in strategic sectors like Earth observation (Group on Earth Observations – GEO; Committee on Earth Observation Satellites – CEOS), exploration of the universe (International Space Exploration Coordination Group – ISECG), Medicine and Microgravity (International Space Life Sciences Working Group – ISLSWG), the analysis of space debris (Inter-Agency Space Debris Coordination Committee – IADC), satellite navigation (International Committee on Global Navigation Satellite Systems – ICG) and security” (ASI 2016).

Concerning security and defense, the Italian White Paper for International Security and Defence from 2015 regards space as “a strategic element for preserving the safety of the ‘national system’ and increases the solidity of the political, economic and social structures” (Italian Ministry of Defence 2015). In addition, the Plurennial Programmatic document (*Documento Programmatico Pluriennale* – DPP) that provides the multiyear plan of the Italian Defence, includes investments to be made in the space component (Italian Ministry of Defence 2018). Space funding includes €212 million in the Cosmo SkyMed second-generation synthetic aperture radar satellite over 4 years and €18,4 million in the Multinational Space-based Imaging System (MUSIS) – Common Interoperability Layer over the 3 years covered by the DPP.

## Spain

### Space and Security Status

Spain is not a permanent member of the UN Security Council. Spain is not a member of the G7 but is invited as a permanent guest member to the G20. Spain has been a member of NATO since 1982. Spain is a member of EDA and SatCen. Spain joined OCCAR in 2005. Spain became ESA Member State in 1979. In Spain, the Ministry of Economy and Enterprise (*Ministerio de Economía y Empresa*) is in charge of drafting and implementing government policy on economic matters and reforms, including space affairs.

### Space and Security Elements in Strategic Documents

The Royal Decree 278/1995 of 24th February 1995 on space exploration, established the Registry of Objects Launched into Outer Space as provided for in the Convention adopted by the United Nations General Assembly on 12 November 1974 (Spanish Prime Minister’s Chancellery 1995).

The 2013 National Security Strategy acknowledges that outer space has become a domain where confrontation is possible (Spanish Government 2013). In addition, the 2015 Ministry of Defence Master Plan of Space Systems highlights the importance of space capabilities for the development of military operations (Spanish Ministry of Defence 2015). This master plan proposes a set of actions to guarantee the maintenance of the existing space capabilities (communications, observation of the earth, navigation and positioning). In addition, it has classified space systems in the

following four families: communication – earth observation – navigation and positioning – surveillance and monitoring. From a technological and industrial point of view, it emphasizes the importance of maintaining effective coordination between public institutions and between these institutions with the industry, avoiding duplications to optimize the benefits from the made investments (Spanish Ministry of Defence 2015).

The 2017 IDS (infodefensa) R&D strategic approach for the defense industry stresses that “it is possible that new programs in other areas, such as space, unmanned aircraft, in-flight refueling aircraft and electronic warfare [...] will be implemented in the short term, and that they will undoubtedly represent an opportunity for Spanish companies” (IDS 2017). The Spanish space industry is primarily involved in contracts of high added value in the areas of qualification of flight and ground equipment and the development and operation of satellite systems. There are also several space centers located in Spain, the most important being namely the European Space Astronomy Centre (Madrid), the Madrid Deep Space Communication Complex (NASA), and Boeing’s European Centre for Research and Technology (also located in Madrid).

## **The United Kingdom**

### **Space and Security Status**

The UK will hold the presidency of the G7 in 2021. The UK was one of the founding members of the NATO in 1949. Brexit has ended British obligations that include permanent involvement in the institutional structures and decision-making processes of the Common Foreign and Security Policy (CFSP) and The Common Security and Defence Policy (CSDP) in the EU. However, this does not automatically preclude any future involvement in defense and security cooperation. The UK is not involved in the Permanent Structured Cooperation (PESCO) in the field of defense. The UK is a permanent member of the UN Security Council and a member of the G7 and G20. The UK is currently a member of EDA and SatCen. It is also a member of OCCAR. The UK has developed strategic alliances with various international partners through multilateral and bilateral cooperation. Since the 1940s, the UK and the USA have been close military allies relishing the so-called the Special Relationship. The UK was one of the founding member states of the ESA in 1975. The Department for Business, Enterprise, and Industrial Strategy (BEIS) is the parent department of UK Space Agency and has the lead for space affairs in the UK.

### **Space and Security Elements in Strategic Documents**

The 1986 Outer Space Act governs and regulates national space activities, including launch and operations of space objects. The Outer Space Act 1986 is the legal basis for the regulation of activities in outer space carried out by organizations or individuals established in the UK or one of its overseas territories or crown dependencies (UK Government 1986).

The UK Government published the National Security Strategy and the Strategic Defence and Security Review: “A Secure and Prosperous UK,” on 23 November 2015 (UK Government 2015a). The two documents comprise the Government’s strategic decisions on defense and security. The former focuses on the country’s “ends” or objectives, while the latter addresses the “ways” and “means” to achieve them. The Strategic Defence and Security Review 15 key investments include the establishment of a Space Operations Control Centre and *Skynet 5 Beyond Line* of sight satellite communications before 2025, and the upgrade of the Space Operations Control Centre and investment in the next generation of secure strategic communications after 2025. Accordingly, the Royal Air force will improve its capabilities in Space Surveillance and Tracking (SST). It will also develop a high-altitude communication relay capability. The Joint Forces Command will provide new satellite communications and “future proof” the navigation and targeting services based on space assets (UK Government 2015a).

Space is an official part of the UK’s critical national infrastructure, as declared by the UK Centre for the Protection of National Infrastructure. The UK Air and Space Doctrine recognizes that the UK relies not only on space for its national security interests but also for its economic prosperity (UK Ministry of Defence 2017). UK space capabilities are inherently dual-use, provided that the same environment, technology and infrastructure, are used to meet both military and civil operations. Space services play a pivotal role in contributing to UK national security, the strength of the economy, and the delivery of public services (UK Ministry of Defence 2017). According to the air and space doctrine, space power makes a pivotal contribution to the potency of UK military power, both as an enabling domain and, increasingly, as an operating domain (in its own right). It is also the domain which makes the most significant contribution to the effectiveness of all the instruments of national power. Space power is defined as “exerting influence in, from, or through, space.” Diplomatic, military and economic credibility, together with a coherent strategy, play a large part in the ability to influence (UK Ministry of Defence 2017).

The Ministry of Defense is expected to release its first dedicated defense space strategy, a plan in line with its ambition for developing and improving Britain’s military space capabilities. The ministry outlined four objectives which may become the guiding priorities of the DSS later this year: “to enhance the resilience of space systems; to improve operational effectiveness; to enhance space support to frontline troops; and to support wider government activities” (UK Ministry of Defence 2019).

Furthermore, the Strategic Defense and Security Review called for a ministerial committee on security and prosperity and the development of the UK National Space Policy. The mandate included the process to “mitigate space weather impacts, improve forecasting, protect the space environment by using civil and military capability, work with international partners, recognize the criticality of satellite navigation, need for enhanced resilience, and innovation in the field of resilient satellite communications” (UK Government 2015a). The Strategic Review refers to the December 2015 UK National Space Policy which has a dedicated section on safety and security of space (UK Government 2015b).

The overarching 2015 National Space Policy links the UK civil space strategy (July 2012) with the National Space Security Policy (April 2014). It aligns with the UK Government's Science and Innovation Strategy and the National Security Strategy. In addition, the 2015 updated Space Innovation and Growth Strategy sets out a partnership between industry, government and academia in order to develop, grow and exploit new space-related opportunities. The 2015 National Space Policy clearly articulates cross-government reliance on space-enabled capabilities. Space is the environment which makes the most significant contribution to the effectiveness of all the instruments of national power (UK Government 2015b).

Finally, the UK Space Agency published in October 2013 a strategy for earth observation from space (2013–2016) in the context of the National Space Policy, the National Space Security Policy (April 2014), and expands on the themes of the UK Civil Space Strategy (July 2012). The strategy concentrates on civil Earth observation requirements but recognizes that some civilian space systems could be dual-use in nature and be capable of supporting national security requirements (UK Space Agency 2013).

---

## Priorities and Trends in National Space and Security/Defense Strategies

Security and defense-related aspects of space activities cover a wide range of activities, mainly divided into two categories: priorities for security *from* space and priorities for security *in* space.

The “Security from Space” priorities consist of disaster management, resource management, transport and communications, environment, climate change and sustainable development, external security including foreign policy and border surveillance, internal security including support to justice and home affairs, military, and financial. The “Security in Space” priorities consist of defensive space security and control, offensive space security and control, space surveillance and tracking, space weather, near earth objects, orbital debris mitigation, space traffic management, active debris removal, and access to space.

The European countries' military space capability priorities point toward several key areas in line with the identified priorities for space in the frame of the EDA Capability Development Plan 2018. National defense strategies and policies define satellite systems as critical infrastructure (enabling domain) and identify space as a separate operating domain. Military operations are inconceivable without the support of space-based systems. Space-based assets and applications are essential to navigation, communication, meteorological, and imagery services, early warning and ballistic missile interception. Space systems make a decisive contribution to the ability to conduct an effective foreign and security policy and to achieve whole-of-government security preparedness including defense aspects in a holistic approach. Strategies and policies increasingly call for the full exploitation of synergies between civil and military developments and dual-use technologies when further developing system capabilities and strategically important key technology competences.

What is more, space is perceived as a domain of socioeconomic development and is essential for security and defense. The list of operational capabilities, required for a coherent and full-spectrum force model include inter alia: IMINT, ELINT, C2, and the protection and security of space assets. SSA underpins all other space roles, as it provides an understanding of the space environment. It enables the timely assessment of and response to space threats, risks, and events, both natural and man-made. Defense White Papers and Strategies are explicitly referring to the increasing threats from space debris promulgation, space weather, offensive space weaponry, as well as the inherent vulnerability of space-based systems from interference and cyber-attacks. In this context, multiple member states are in the process of elaborating dedicated space defense strategies and revising their organizational structures.

---

## Conclusion

This chapter provides evidence of the trend towards increasing relevance for security and defense in national space policy initiatives of the presented European countries. The identified national space, security, and defense strategies demonstrate an evolution of European states priorities to dual-use utilization. The policy developments at national level, in combination with the recent EU and ESA policy-making initiative, recognize the important role of space for security and defense. They also demonstrate the increasing relevance of security and defense in Europe, in general, which to some extent could be framed as the necessity for Europe to further enhance its own security and defense.

**Disclaimer** The contents of this chapter and any contributions to the Handbook reflect personal opinions and do not necessarily reflect the opinion of the European Space Agency (ESA).

---

## References

- CNES (2015) *Ambition 2020–2015, Space for climate*. Available at: [http://www.cnes-csg.fr/automne\\_modules\\_files/standard/public/p11636\\_99f9990e67f7bbf293ff282b37d9bc1eCNES\\_plk\\_instit\\_2015\\_171214\\_GB.pdf](http://www.cnes-csg.fr/automne_modules_files/standard/public/p11636_99f9990e67f7bbf293ff282b37d9bc1eCNES_plk_instit_2015_171214_GB.pdf)
- Euractiv (2019) NATO braces for the new space age, 21 November 2019. Available at: <https://www.euractiv.com/section/global-europe/news/nato-braces-for-the-new-space-age/>
- European Commission (2018) Proposal for a regulation of the European Parliament and of the Council establishing the space programme of the union and the European Union Agency for the space programme and repealing regulations (EU) No 912/2010, (EU) No 1285/2013, (EU) No 377/2014 and Decision 541/2014/EU, COM(2018) 447 final 2018/0236 (COD), 6 June 2018, Brussels. Available at: [https://ec.europa.eu/commission/sites/beta-political/files/budget-june2018-space-programme-regulation\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/budget-june2018-space-programme-regulation_en.pdf)
- French Ministry for the Armed Forces (2013) *French White Paper on Defence and National Security and Bill on Military Planning 2014–2019 (updated 2019–2025)*. Available at: <https://www.defense.gouv.fr/english/dgris/defence-policy/white-paper-2013/white-paper-2013>



- French Ministry for the Armed Forces (2017) Strategic Review of Defence and National Security of 13 October 2017. Available at: <https://www.defense.gouv.fr/english/dgris/defence-policy/strategic-review-of-defence-and-national-security-2017/strategic-review>
- French Ministry for the Armed Forces (2019) Space defence strategy, Report of the “Space” working group, July 2019. Available at: <https://www.defense.gouv.fr/english/dgris/defence-policy/defence-strategy/defence-strategy>
- French Republic (2008) Law concerning space operations – *Loi sur les Opérations Spatiales* (French Space operations act). Available at: <https://www.unoosa.org/pdf/pres/lsc2009/pres-04.pdf>
- French Republic (2012) French space strategy (*Stratégie spatiale française*). Available at: <https://www.vie-publique.fr/sites/default/files/rapport/pdf/124000161.pdf>
- French Republic (2015) National strategy for the security of maritime areas – Adopted by the inter-ministerial sea committee on 22 October 2015. Available at: [https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2016/01/strategie\\_nationale\\_de\\_surete\\_des\\_espaces\\_maritimes\\_en\\_national\\_strategy\\_for\\_the\\_security\\_of\\_maritime\\_areas.pdf](https://www.gouvernement.fr/sites/default/files/contenu/piece-jointe/2016/01/strategie_nationale_de_surete_des_espaces_maritimes_en_national_strategy_for_the_security_of_maritime_areas.pdf)
- German Federal Government (2016) White paper on German security policy and the future of the Bundeswehr. Available at: <http://www.gmfus.org/publications/white-paper-german-security-policy-and-future-bundeswehr>
- German Federal Government (2018) High-tech strategy 2025. Available at: [https://www.bmbf.de/upload\\_filestore/pub/The\\_High\\_Tech\\_Strategy\\_2025.pdf](https://www.bmbf.de/upload_filestore/pub/The_High_Tech_Strategy_2025.pdf)
- German Federal Ministry of Economics and Technology-BMWi (2010), Making Germany’s space sector fit for the future – the space strategy of the German Federal Government, November 2010. Available at: [https://www.dlr.de/rd/en/Portaldata/28/Resources/dokumente/Raumfahrtstrategie\\_en.pdf](https://www.dlr.de/rd/en/Portaldata/28/Resources/dokumente/Raumfahrtstrategie_en.pdf)
- German Federal Ministry of Justice (1990) Law governing the transfer of responsibilities for space activities of 8 June 1990 as amended. Available at: [http://www.esa.int/About\\_Us/ECSL\\_European\\_Centre\\_for\\_Space\\_Law/National\\_Space\\_Legislations](http://www.esa.int/About_Us/ECSL_European_Centre_for_Space_Law/National_Space_Legislations)
- German Federal Ministry of Justice (2007) Satellite data security act. Available at: [https://www.bmwj.de/Redaktion/DE/Downloads/S-T/satdsig-hintergrund-en.pdf?\\_\\_blob=publicationFile&v=1](https://www.bmwj.de/Redaktion/DE/Downloads/S-T/satdsig-hintergrund-en.pdf?__blob=publicationFile&v=1)
- Giannopapa C, Adriaensens M, Antoni N, Schrogl K-U (2018) Elements of ESA’s policy on space and security. *Acta Astronaut* 147:346–349
- Italian Ministry of Defence (2015) White Paper for International Security and Defence, 2015. Available at: <http://www.iai.it/sites/default/files/iaiwpl1734.pdf>
- Italian Ministry of Defence (2018) Pluriennial Programmatic document (Documento Programmatico Pluriennale, DPP). Available at: <https://www.iai.it/en/pubblicazioni/italys-defence-expenditure-what-impact-eu-defence-cooperation>
- Italian Parliament (2018) Space bill containing measures for the coordination of the space and aerospace policies along with important regulations concerning the organization and functioning of the Italian Space Agency-ASI. Available at: <https://www.altalex.com/documents/leggi/2018/02/14/misure-per-il-coordinamento-della-politica-spaziale>
- Italian Presidency of the Council of Ministers (2019) National Security Strategy for Space, July 2019. Available at: [http://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/UfficiDiretta\\_CONTE/COMINT/NationalSecurityStrategySpace.pdf](http://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/UfficiDiretta_CONTE/COMINT/NationalSecurityStrategySpace.pdf)
- Italian Prime Minister’s Office (2019) Government guidelines on space and aerospace, March 2019. Available at: [http://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/UfficiDiretta\\_CONTE/COMINT/DEL\\_20190325\\_aero-spazio-EN.pdf](http://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/UfficiDiretta_CONTE/COMINT/DEL_20190325_aero-spazio-EN.pdf)
- Italian Space Agency – ASI (2016) Strategic vision document 2016–2025. Available at: <https://www.researchitaly.it/en/projects/space-strategic-vision-2016-2025-document-published-by-asi/>
- Japan Space Forum (2015) The German interagency approach to SSA, presentation, 2015 Japan Space Forum SSA symposium

- NATO (2019) Defence expenditure of NATO countries (2013–2019) press release, PR/CP (2019) 123, November 2019. Available at: [https://www.nato.int/cps/en/natohq/news\\_171356.htm](https://www.nato.int/cps/en/natohq/news_171356.htm)
- Papadimitriou A, Adriaensen M, Antoni N, Giannopapa C (2019) Perspective on space and security policy, programmes and governance in Europe. *Acta Astronaut* 161:183–191
- Spacewatch.Global (2019) first EU-ESA Space Council in Eight Years Held, discusses Space as enabler, 28 May 2019. Available at: <https://spacewatch.global/2019/05/first-eu-esa-space-council-in-eight-years-held-discusses-space-as-enabler/>
- Spanish communication company specialized in Defence and security – IDS (infodefensa) (2017) Spain Defence & Security Industry, R&D, the strategic approach 2017. Available at: [https://www.infodefensa.com/archivo/files/spain2017\(ing\)OK%20.pdf](https://www.infodefensa.com/archivo/files/spain2017(ing)OK%20.pdf)
- Spanish Government (2013) The National Security Strategy – sharing a common project. Available at: [https://www.lamoncloa.gob.es/documentos/estrategiaseguridad\\_baja\\_julio.pdf](https://www.lamoncloa.gob.es/documentos/estrategiaseguridad_baja_julio.pdf)
- Spanish Ministry of Defence (2015) Master plan of space systems. Available at: <http://www.defensa.gob.es/Galerias/dgamdocs/plan-director-sistemas-espaciales.pdf>
- Spanish Prime Minister's Chancellery (1995) Royal Decree No. 278/1995 of 24 February 1995, Establishment in Spain of the Registry of Objects Launched into Outer Space as provided for in the Convention adopted by the United Nations General Assembly on 12 November 1974. Available at: [http://www.unoosa.org/oosa/en/ourwork/spacelaw/nationalspacelaw/spain/royal\\_decree\\_278\\_1995E.html](http://www.unoosa.org/oosa/en/ourwork/spacelaw/nationalspacelaw/spain/royal_decree_278_1995E.html)
- UK Government (1986) Outer space act. Available at: [http://www.unoosa.org/res/oosadoc/data/documents/2017/aac\\_105c\\_12017crp/aac\\_105c\\_12017crp\\_21\\_0\\_html/AC105\\_C1\\_2017\\_CRP21E.pdf](http://www.unoosa.org/res/oosadoc/data/documents/2017/aac_105c_12017crp/aac_105c_12017crp_21_0_html/AC105_C1_2017_CRP21E.pdf)
- UK Government (2015a) National Security Strategy and Strategic Defence and Security Review 2015-A Secure and Prosperous United Kingdom, November 2015. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/478933/52309\\_Cm\\_9161\\_NSS\\_SD\\_Review\\_web\\_only.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/478933/52309_Cm_9161_NSS_SD_Review_web_only.pdf)
- UK Government (2015b) National Space Policy., 13 December 2015. Available at: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/484865/NSP\\_-\\_Final.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/484865/NSP_-_Final.pdf)
- UK Ministry of Defence (2017), Joint Doctrine Publication 0–30 (JDP 0–30) – UK Air and Space Power, December 2017. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/668710/doctrine\\_uk\\_air\\_space\\_power\\_jdp\\_0\\_30.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668710/doctrine_uk_air_space_power_jdp_0_30.pdf)
- UK Ministry of Defence (2019) Towards a defence space strategy. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/712376/MOD\\_Pocket\\_Tri-Fold\\_-\\_Defence\\_Space\\_Strategy\\_Headlines.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/712376/MOD_Pocket_Tri-Fold_-_Defence_Space_Strategy_Headlines.pdf)
- UK Space Agency (2013) Strategy for earth observation from Space 2013–16, October 2013. Available at: [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/350655/EO\\_Strategy\\_-\\_Finalv2.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/350655/EO_Strategy_-_Finalv2.pdf)



Małgorzata Polkowska

## Contents

Introduction .....	486
The Polish Space Agency (POLSA) .....	486
Strategic Priorities in Space Law and National Security and Defense .....	487
Polish Security and Defense Strategy .....	487
Polish Space Law and Space Strategy .....	489
National Programs .....	490
Multilateral Programs .....	492
Bilateral Cooperation .....	492
European Union SST Consortium and Role of Poland .....	493
ESA and Poland .....	496
Conclusions .....	497
Acknowledgement .....	497
References .....	497

## Abstract

The main objectives of this chapter are to address the importance of space security in Poland, as mainly demonstrated through the activities of the Polish Space Agency (POLSA). This agency has played an important role in the Space Situational Awareness (SSA) program for safety and security purposes. Poland decided to put in place an SSA system as part of the national and regional security law and policy. The proper implementation of the SSA program is necessary for all states. Poland, as a full member of the European Space Surveillance and Tracking (SST) Consortium, is willing to participate in European projects. Thus, the regional and multilateral cooperation in this matter is crucial.

---

M. Polkowska (✉)  
University of War Studies, Warsaw, Poland  
e-mail: [m.polkowska@akademia.mil.pl](mailto:m.polkowska@akademia.mil.pl)

---

## Introduction

Space security has always been an important component of national policy. The Space Situational Awareness system is crucial for a state's security, as well as for its international responsibility to implement it correctly into national policy and law. This chapter presents some legal challenges occurring in this process within the European Union, with particular emphasis being put on Poland. The proper governance of space security is important for states, not only at international but also at regional and national level. That is why the role of the national regulator should be significant in incorporating space security in the policy and strategy of the state. Regular cooperation between states at international and bilateral level is necessary. Although Poland is not a major space-faring nation, the security issue has always been treated as a priority.

---

## The Polish Space Agency (POLSA)

Poland has become more and more active in space and also in space security, in particular since the Polish Space Agency (POLSA) was created. This agency is a governmental executive body, subject to the Prime Minister. It consists of civilian and military personnel. POLSA was established by the Act of 26 September 2014 and became fully operational at the end of 2015 (Polish Government 2014). The agency participates in fulfilling the strategic goals of the Republic of Poland by supporting the utilization of satellite systems and the development of space technologies. The main tasks of POLSA cover the following five areas: coordinate the activity of the Polish space sector at national and international level; represent Poland in relation to international space sector organizations; support national science and business projects associated with space technologies; popularize the use of satellite data by public administration; and increase the defensive capabilities of the country. The agency is executive in nature in accordance with the Act of 27 August 2009 on public finance (art. 1.1 – Act of 26 September 2014), and it can create local branches. The headquarters of the agency are located in Gdansk (Art. 1 par. 3).

The activities of the agency are under the auspices of the President of the Council of Ministers (Art. 2). The duties of the agency are written in Art. 3. The POLSA Council consists of representatives of the government – one from each administration and four representatives of scientists and the industry with recognized achievements in research or business – which are chosen based on their knowledge competence in areas concerning POLSA activities (Art. 14) (Polkowska 2016). One of the main areas of POLSA activities is international cooperation. POLSA is committed to multilateral cooperation in the framework of the European Space Agency (ESA) and the European Union (EU). POLSA supports especially Polish actors who apply to the space programs. They have already started efforts to

integrate the national industrial sector in projects implemented by the European Organization for the Exploitation of Meteorological Satellites (EUMETSAT). POLSA provides also active bilateral cooperation with ESA Member States, the EU, and other countries, primarily in the field of space exploration.

POLSA supports the Polish space sector and facilitates exchanges, by organizing competitions for advisory services. The entities receive professional support in the form of consultation with experts. Entrepreneurs from SMEs receive support in applying to competitions organized by the European Space Agency. POLSA activities aim at contributing to the growth of innovation and competitiveness of Polish companies in the space sector. POLSA encourages the involvement of high-tech or IT operators in the space industry, and it also promotes solutions supporting the Polish state administration at central and local government. This results in enhanced efficiency of the administrative work by using everyday services based on satellite data and satellite technology, including Earth observation, navigation, and telecommunications. With regard to Research and Development (R&D), POLSA supports the Polish scientific institutions and companies who are active in R&D in the field of fundraising for scientific and industrial research. POLSA assists in conducting work on space applications and space technology development.

In addition, POLSA carries out educational activities in the field of popularization of knowledge of space research at secondary education and high school in Poland. It covers the subject of space engineering and astronomy, as well as it initiates and supports with its expertise the creation of new courses of higher education. Last but not least, one of the main priority tasks of the Polish Space Agency is to provide security for Poland and its citizens by increasing Polish defense capabilities through the use of satellite systems. To this direction, the Polish Space agency aims to ensure the security of the state and its citizens and to contribute to the Polish defense potential through the use of satellite systems. Therefore, an important area of the agency's activity is the coordination of activities aimed at the effective use of space technologies and satellite applications for defense purposes.

---

## **Strategic Priorities in Space Law and National Security and Defense**

### **Polish Security and Defense Strategy**

The tasks resulting from the abovementioned priorities are carried out by the Vice President's Division for Defense Affairs. The Division consists of the Department of Military Satellite Technologies and the Department of Defense Projects. The Military Satellite Technologies Department consists of the Earth and space satellite recognition team, the satellite navigation team, and the satellite communications team. The Military Satellite Technologies Department is responsible for the following tasks (Polish Space Agency [www.polsa.gov.pl](http://www.polsa.gov.pl)):

- Use of satellite products and services for national security and defense; ensuring the state's capacity in the field of Earth observation, satellite navigation, and satellite communications, in particular for the needs of the Armed Forces of the Republic of Poland
- Identification of military needs in the field of satellite and space technologies and recommendation of their implementation within the framework of the plan for technical modernization of the Polish Armed Forces
- Cooperation with the institutions within the Ministry of National Defense who manage military equipment in the field of Earth observation, communication, and satellite navigation, including the determination of the scope of this cooperation
- Developing concepts for the development and application of satellite technologies for national security and defense, including the development of documentation for the preparation of feasibility studies
- Analyzing and issuing opinions on projects prepared and implemented by Polish entities for national and international programs within the framework of military satellite technologies from the technical point of view
- Monitoring and analyzing progress in the global development of satellite technologies and methods, as well as supporting Polish scientific, research, and industrial entities that develop satellite technologies for potential application in the Armed Forces of the Republic of Poland

The Department of Defense Projects has the following responsibilities:

- (a) Supporting the needs of the Polish Armed Forces and other bodies and institutions responsible for national security through:
  - Implementation of programs and projects as well as management of scientific research or development works aimed at acquiring new technologies for the purposes of national defense and security
  - Monitoring defense and security programs and projects while developing recommendations on how to manage their effects in order to achieve new capabilities resulting from space exploration and development of satellite technologies
  - Preparation of analyses, reports, recommendations, and advice in the field of space exploration, as well as the use of space and space technologies for national defense and security purposes
  - Representation of national defense and security interests in the area of space exploration and uses of outer space
- (b) Increasing Poland's participation in international programs of significance for the national defense and security objectives through:
  - Activities aimed at the increasing involvement of scientific centers, research centers, industry, and the Ministry of National Defense in international programs

- Supporting, in consultation with the Minister of National Defense, the representation of national defense interests in the field of space exploration and use in international programs
- Participation in the consultation process concerning Polish activity in the field of space exploration and use for defense purposes, including by appointing advisors and experts to Polish delegations and representations in European Union institutions and bodies of international organizations, in particular ESA, EDA, and NATO
- Monitoring activities in the field of initiatives and participation of the Polish Armed Forces in international programs
- Taking care of the cohesion of the Polish space policy within the framework of implemented international programs and recommending the possibility of implementing the effects of this cooperation
- Supporting works aimed at preparing and updating the National Space Sector Development Program

## Polish Space Law and Space Strategy

Poland is very active in developing a policy and legal framework concerning space security and Space Surveillance and Tracking (SST). In February 2017 the Polish Space Strategy, published by the Polish Ministry of Economic Development, entered into force (Polish Space Agency [www.polsa.gov.pl](http://www.polsa.gov.pl)). The objectives stipulated in the strategy include, among others, increasing the competitiveness of the Polish space sector and its share in turnover (increasing participation in the EU space programs through the EU SST Consortium); development of satellite applications; strengthening capacities in the area of security and defense using space (establishment of SSA); and creating favorable conditions for the development of space sector in Poland or building resources for the Polish space sector. The strategic aim is to obtain 3% of the EU market in 2030.

In 2018 the National Space Plan was established for the years 2019 and 2021 ([www.polsa.gov.pl](http://www.polsa.gov.pl)). One of the main ambitions is the establishment, development, and operation of national Space Situational Awareness (SSA) system in relation to the EU SST Consortium. The objective of the project is to enhance the security of citizens and infrastructure (Earth and space) in the context of space threats, to build national SSA capabilities, and to prepare for commercial exploitation of services provided in the area of SSA. The first phase of the activity is to launch basic functions of the national SST system, inter alia, through the development of infrastructure and capabilities enabling the implementation of tasks envisaged within the framework of Poland's future membership in the European SST Consortium. On 19 December 2018, Poland joined the European SST Consortium related to the tracking of space debris threatening infrastructure in space and on Earth (Polkowska 2019, Malacz et al. 2018).

The Polish Space law is still waiting for parliamentary approval. Several versions of the draft have been developed. Currently, the Government Legislation Centre

website has published a draft law on the regulation of space activities and the National Register of Space Objects (Polish Government, Government Legislative Process <https://legislacja.rcl.gov.pl/>). Earlier, however, the amendment of the Act on POLSA will be processed. The changes proposed in the draft act aim to clarify the scope of the Polish Space Agency's tasks, as an executive agency that provides the expertise and technological knowledge to other public administration bodies involved in space activities and is responsible for the preparation and coordination of the National Space Program implementation; adapt the supervision of POLSA to the solutions in place in other European countries, especially in the Member States of the European Space Agency (ESA); as well as introduce improvements in the organization of POLSA.

---

## National Programs

In December 2018 the Polish National Space Program was introduced. At the moment it is still in public consultations. The Polish Space Agency (POLSA) will be responsible for the implementation of the program. POLSA has considered a few areas of public support within the program, such as "Development of satellite systems" – with one of the priority projects being the "Space Situational Awareness" system. The vital goal of the project is to ensure a long-term access to the European and national space infrastructure by providing services crucial for securing its operations. As a consequence, a network of sensors (telescopes, lasers, radars) responsible for space object observation and tracking will function on the territory of Poland, and personnel will be trained in order to perform tasks in the frame of SST (Polkowska 2019). Poland is very motivated to follow the European legislation steps and supports EU activities at the SSA level. Poland joined the European SST Consortium related to the tracking of space debris threatening the infrastructure in space and on Earth. At the end of 2018, Poland became a full member of the European Space Surveillance and Tracking Consortium. The accession agreement was signed on 19 December 2018 at the seat of the Polish Space Agency in Warsaw. Joining the consortium will enable national entities to participate in projects financed by the European Union, whose budget in the current and future financial perspective may amount to more than EUR 350 million.

Membership in the consortium will allow for faster development of the Polish SST system, which will provide Poland with data necessary to protect the planned missions of Polish satellites and will support national security and defense in monitoring threats from artificial space objects. Participation in the European program also brings great scientific and business potential. Ensuring the operability of the observation sensors forming the Polish SST infrastructure, the possibility of their modernization, and the demand for new ones – all this will facilitate a faster growth of competence in the area of SST and optical and radar observations for Polish entities, which already today gain experience by implementing projects under the optional SSA program in ESA.



Starting from 2019 Poland, as a full member of the SST Consortium, shares benefits from services at national level and especially adapts nationally to the possible future contribution. That is why to both stimulate and secure the economic growth and to protect European citizens, there is a strong need for continuous dialogue to improve the boundaries for a more comprehensive future Space Situational Awareness program. Joining the SST Consortium will allow to enhance national capabilities related to observation and awareness building in space, increase the national space sector competences and their role in current and future programs of the European Union and the European Space Agency, as well as strengthen Poland's position in the international arena. Therefore, the establishment, development, and exploitation of the national system of situational awareness in space has been included as one of the five large projects in the National Space Program for the years 2019–2021.

Poland – as a member of the SST Consortium – will ensure the use of a number of telescopes located worldwide (including Poland, Argentina, Australia, Chile, South Africa, and the USA) belonging to:

The Nicolaus Copernicus Astronomical Center of the Polish Academy of Sciences with research groups: High Energy Astrophysics, Stellar Astrophysics, etc.

The Adam Mickiewicz University Astronomical Observatory Institute in Poznań: research on dynamics of artificial satellites and space debris or optical observations and laser ranging of artificial satellites and space debris

The Baltic Institute of Technology Research Foundation in Gdynia: robotic telescopes for the detection and monitoring of space debris and satellites and companies

The Sybilla Technologies: a software development company and integrator of turn-key robotic optical observatories, specializing in the “from sensor to TDM” chain of SST services

The 6ROADS: a focused company that owns and operates a global network of telescopes to provide high-quality data in the SST domain

The infrastructural core of 6ROADS is composed of six optical observatories located across the globe. As a company 6ROADS was established in 2016, although its experience can be traced back to 2003 and the laser station of the Space Research Centre of the Polish Academy of Sciences from the Observatory in Borowiec. The Borowiec satellite laser ranging station belongs to the Space Research Centre of the Polish Academy of Sciences (SRC PAS), and it is the only such device in Poland and one of the few ones in the world working since the mid-1980s. The Borowiec satellite laser ranging station (CSLRB) started to track typical space debris targets, cooperative inactive/defunct satellites, and uncooperative rocket bodies in the middle of 2016. Currently, the station is actively involved in the development of the Space Surveillance and Tracking program, developed by European Space Agency (Space Safety program), as well as programming tools and competences related to the processing and analysis of SST data (Polish Space Sector catalogue of selected entities, POLSA 2018 and Konacki et al. 2019).

## Multilateral Programs

### Bilateral Cooperation

In April 2019 during the 35th Space Symposium in Colorado Springs, POLSA signed an agreement with US Strategic Command (USSTRATCOM) for sharing SSA data. Due to this agreement, Poland will gain access to Space Situational Awareness services and data, including alerts concerning collisions, fragmentation, or uncontrolled satellite reentries into the Earth's atmosphere. The data will be provided by the US Air Force Space Command's 18th Space Surveillance Squadron on the basis of the agreement signed. Poland joins 18 nations (the Netherlands, Brazil, the UK, the Republic of Korea, France, Canada, Italy, Japan, Israel, Spain, Germany, Australia, Belgium, the United Arab Emirates, Norway, Denmark, Thailand, and New Zealand), 2 intergovernmental organizations (the European Space Agency and the European Organization for the Exploitation of Meteorological Satellites), and more than 77 commercial satellite owners, operators, and launchers already participating in SSA data-sharing agreements with USSTRATCOM (US Embassy and Consulate in Poland <https://pl.usembassy.gov/ssa/>). The collaboration falls within areas of SWE, NEO, and SST.

Poland understands the SSA influence on national security in space, which is a priority for Polish politicians and legislative bodies. In October 2019 the leaders of POLSA and the US National Aeronautics and Space Administration (NASA) signed a landmark Joint Statement of Intent for Space Cooperation during the 70th International Astronautical Congress in Washington, D.C. This agreement highlighted the countries' respective interests in cooperative human and robotic space exploration in all spheres.

During just the past 40 years, over 80 instruments designed and constructed by Polish scientists and engineers have been employed in various international space missions, and 7 years of participation in the European Space Agency (ESA) have resulted in the dynamic development of the Polish space sector, in which more than 350 Polish enterprises operate. These companies and institutions cooperate with ESA and other national agencies, including NASA, DLR (German Space Agency), JAXA (Japanese Aerospace Exploration Agency), and CNSA (China National Space Administration). These include several sensors and robotic probes on NASA's Mars Curiosity and InSight landers, among other significant accomplishments.

Poland has established relations with European states as well in space. In 2000 started the relations with EUMETSAT as a cooperating member and gained full membership in 2009. The Act on Ratification of the Convention on the Establishment of the European Organization for the Exploitation of Meteorological Satellites (EUMETSAT) drawn up in Geneva on 24 May 1983 was adopted by the Parliament of the Republic of Poland on 9 January 2009. The Institute of Meteorology and Water Management, the National Research Institute, is responsible for relations with the organization and participates in the work of EUMETSAT bodies. Thanks to its membership in the organization, Poland has full access to satellite data from its

satellites. The images provided by EUMETSAT are primarily used by the state hydrological and meteorological services to prepare forecasts, hydrometeorological protection of society and economy, and monitoring of climate change by the Polish Armed Forces, universities, and research institutes. Images from meteorological satellites may also be used in agriculture, forestry, land management, spatial management, investment planning, and monitoring of water areas (including the Baltic Sea) and atmosphere, including, among others, trace gas and aerosol measurements. Furthermore, the Polish Institute of Geodesy and Cartography is collaborating in the project COSMO-SkyMed.

## **European Union SST Consortium and Role of Poland**

The European SST Support Framework related to detection, tracking, and monitoring of orbital movements of active and inactive satellites and space debris is a key operational program of the European Union in the space area, in addition to the Galileo satellite navigation program and the Copernicus Earth observation program. The initiative is based on the 2014 Decision of the European Parliament and the Council of the European Union to establish a Space Observation and Tracking Support Framework to contribute to the long-term availability of European and national space infrastructure and services necessary for the security of Europe's economy, society, and citizens (Decision No 541/2014/EU of the European Parliament and of the Council of 16 April 2014 establishing a Framework for Space Surveillance and Tracking Support, 27.5.2014, L 158/227.).

The main objectives of the SST program concern assessing and reducing the risks to European spacecraft launches and operations resulting from possible collisions; studies, assessments, and warnings against uncontrolled entry into the atmosphere of space objects and debris threatening the safety of citizens and ground-based infrastructure; or exploring ways of preventing the spread of space debris (Polish Space Agency <https://polsa.gov.pl/en/>). The European SST program related to the detection, tracking, and monitoring of orbital movement of active and inactive satellites and space debris is a key operational program of the European Union in the space area, alongside the Galileo satellite navigation program and the Copernicus Earth observation program. In 2015 the European Commission set up the SST Consortium to coordinate this initiative, whose task is to pool the capabilities of European countries in order to secure European and national space infrastructure (Faucher 2019).

Member States have contributed to the consortium national optical and radar sensors capable of observing artificial objects moving around the Earth and the ability to analyze the data provided by these sensors. On the basis of processed data, SST services shall be implemented in the form of risk assessment, information, and alerts on actual and predicted space events involving artificial space objects. Such events can be, e.g., collisions and fragmentations of objects in orbit or uncontrolled entry into the Earth's atmosphere of artificial space objects. Information is made available to stakeholders, including EU institutions, Member States, and satellite

operators. Initially, the members of the consortium were leading European countries, Germany, France, Spain, Italy, and the UK, represented mainly by national space agencies. At the end of 2018, Romania, Portugal, and Poland joined the group (Faucher 2019). In view of progressing the commercialization of products related to situational awareness in space, domestic entities providing solutions and services in this area will be able to direct their offer also to the global market, which will grow as a result of the New Space trend, the increasing number of small satellites, the planned development of mega-constellations and new areas such as satellite in-orbit servicing, or, in the longer term, the sourcing of raw materials from celestial bodies (Polish Space Agency <https://polsa.gov.pl/en/>).

Having in mind the provisions of the Space Strategy for Europe and longstanding dialogue in the space domain in Europe, as being performed among others within the SST Committee, Poland supports the SST Support Framework and its further evolution. Space technologies, operational spacecraft, and relevant services are the key elements to sustain, support, and enhance the EU policies, economy, security, and technology leadership which are nowadays already of great importance and undoubtedly will be much more in the future. Poland joining the SST Consortium is the result of several years of activity from the Polish side, including the Ministry of Enterprise and Technology, the Ministry of National Defense, and the Ministry of Science and Higher Education and the Polish Space Agency, which prepared the accession application submitted to the European Commission and, together with specialists from the Ministry of Science and Technology, conducted negotiations on the most favorable membership conditions. As part of the preparatory works of the Polish Space Agency, a feasibility study of the Architecture of the Space Awareness System in Poland (SSA) project was commissioned, with particular emphasis on the space object observation and tracking subsystem (SST).

Participation in the Consortium brings for Poland a number of other obligations of organizational nature (e.g., creation of a network of declared sensors and a national operational center), human resources (e.g., provision of specialists for the functioning of the national SST system), financial (allocation of national resources for the launch of the SST system and absorption of EU funds), and legal obligations (adjustment of the SST system). The first stage of work resulting from Poland's membership in the SST Consortium and provided for in the National Space Program will be to launch basic functionalities of the system based on declared sensors, inter alia, through the development of national infrastructure and capabilities enabling the implementation of tasks and projects within the European SST Consortium and increasing the participation of Polish entities in the SSA (Space Situational Awareness) program of the European Space Agency.

Poland shares the main point of the Commission recognizing the aim of current Decision from 2014 "to ensure the long term availability of European and national space infrastructure facilities and services which are essential for the safety and security of the economies, societies and citizens in Europe" and have a will to extend it to the issues of "sustainable access to space and its usage" and "protection of EU and its citizens against any natural and artificial hazards

coming from space” by the possible intervention in the following domains: Space Surveillance and Tracking (SST), Space Weather (SWE), and Near-Earth Object (NEO). It seems that the future steps of Commission might also consider space traffic management (STM), active debris removal (ADR), and space mining (SM). SST, SWE, and NEO seem to be of high priority as directly influencing safety and security of European citizens and very challenging to tackle at national level. In those areas EU seems to have the necessary prerogatives to take necessary actions on European level. However, SWE and NEO should be considered to be continued and enhanced based on ESA accomplishments and with ESA involvement at least in the Research and Development (R&D) phase. To fulfil the objectives of the current Decision from 2014 and having in mind the magnitude of necessary intervention, Poland is in favor of developing the idea of broadening the current SST Framework Support, eventually like main EU space program as Galileo or Copernicus. Only such an approach may properly correspond to the challenges of contemporary space environment such as (Chimicz 2018):

1. Increase in congested and contested space environment, among others taking into account planned mega-constellations, new space entrants, suborbital flights challenges, maturing, and usage of ASAT technologies
2. Possible incorporation of space into air traffic management
3. Emergence of new industry branches in the domain (e.g., sensors technologies as a commodity, commercialization of SST delivery)
4. Growing interest of space weather for aviation, transport, and other domains
5. Increase of security and defense issues of space
6. Enforcing international regulation and responsible behavior in space (COPUOS and IADC guidelines)

Moreover, in case of financial constraints, it should be considered to use also other tools available to the European Commission to enable a coherent intervention. In practice, the overall program may be accomplished by the main financial line (e.g., SSA) with additional supporting lines for, e.g., SWE/NEO coming from other programs (e.g., Copernicus, Galileo, or H2020). Poland strongly recognizes the two-dimensional aspects of the programs, i.e., the military and civilian. From this perspective the European intervention and existing and future regulations must respect national interests and issues related to sovereignty of countries, in particular the assets ownership, as well as recognize the program as a kind of contribution to European Common Security and Defense Policy. As today's EUSST program should encompass strong cooperation with the USA and parallel allow to include (if applicable) the option to cooperate with other non-EU countries able and willing to contribute to it (e.g., allied nations as well as space faring nations). Additionally, other ways of cooperation between potential EUSST/SSA Consortium member and other EU states (if really profitable) should be considered (EUSST <https://www.eusst.eu>).

## ESA and Poland

ESA is a basic partner for the majority of Polish companies from the space sector. Importance of the cooperation with ESA lies not only on the opportunities of funding development work but also on a large transfer of know-how from ESA to Polish entities such as SAT-AIS-PL, in the frame of which Polish entities build a microsatellite. This work is supervised by ESA experts (Brona 2018). Regarding the trends of the Space 4.0 era, the niches occupied by the Polish space sector are primarily:

- Optical observations
- SSA program systems and subsystems
- SSA data processing software
- Space robotics
- Photonics
- Optoelectronics
- Small satellite systems and subsystems (power supply systems, on-board computers, satellite receivers for GPS and Galileo systems, integrated microwave modules, satellite propulsion systems, and exploration missions)
- EGSE (Electrical Ground Support Equipment) and MGSE (Mechanical Ground Support Equipment) systems
- Aggregation and data processing systems
- EO and GNSS data processing applications

The Polish Space Agency, together with state institutions, takes part in the European Space Surveillance and Tracking (EUSST) clusters and PERASPERA (Plan European Roadmap and Activities for Space Exploitation of Robotics and Autonomy), as well as in the European network ENTRUSTED (Governmental Satellite Communication (GOVSATCOM) program). Additionally, a primary national space-focused project is the SAT4ENVI platform, concerning the operational collection of sharing and promotion of digital satellite information on the environment. Polish companies and research institutes are already implementing ambitious ESA projects developing satellite applications or creating products present in orbit around the Earth and used in scientific missions in the Solar System. Poland allocated a total of EUR 39 million for optional programs, engaging in seven programs: European Exploration Envelope Program (E3P), Space Safety Program, Earth Observation, program of Advanced Research in Telecommunication Systems (ARTES 4.0), Navigation (NAVISP), General Support Technology Program (GSTP), and PRODEX.

Poland will take part in Earth observation programs, which in recent years have proved to be a very popular and fully exploited area for the Polish space sector. Among the optional programs that Poland has decided to support is also the Space Safety Program, which gives Polish companies the opportunity to achieve a high degree of specialization in space security technologies. The Polish Institute of Geodesy and Cartography has launched several projects within ESA. Current projects are ESA EOstat (2018–2020) – Agriculture Poland: Services for Earth Observation-based

statistical information for agriculture (Coordinator: PhD Jędrzej Bojanowski, cooperation: Institute of Geodesy and Cartography, Space Research Centre of Polish Academy of Sciences, Statistics Poland); and ESA IRRSAT (2017–2019) – Irrigation Factor 4 potato growth using Sentinel-1 and Sentinel-2 data (Coordinator: Industrial Institute of Agricultural Engineering, cooperation: IGIK Remote Sensing Centre, WUT Institute of Electronic Systems) (Polish Government, Ministry of Development, Poland on Space 19+, <https://www.gov.pl/web/rozwoj/polska-na-space19—perspektywy-rozwoju-sektora-kosmicznego-na-najblizsze-trzy-lata>).

---

## Conclusions

As it was already mentioned in national strategies, societies increasingly depend on space technologies. Poland and its Space Agency are convinced that security in Space is a crucial issue that needs to be tackled. The practical example of the international use of SSA is the creation of the EU Consortium (with Poland on board), which will require from the Member States internal and external cooperation for security purposes. Due to the fact that Poland is more active in space, security has become more and more important. That is the reason why there is a need for increased cooperation among Member States in Europe and worldwide and information exchange about the best achievable ways forward.

---

## Acknowledgement

This publication was financed under a project implemented in the Research Grant Program of the Ministry of National Defense, Republic of Poland.

---

## References

- Brona G (2018) Mapa rozwoju rynków i technologii dla sektora kosmicznego w Polsce, 2019, Polska Agencja Przedsiębiorczości 2018
- Chimicz A (2018) POLSA, 13th military SSA conference presentation, April 2018, London, enhancing space capabilities for the polish MOD: SSA System Development
- EUSST. <https://www.eusst.eu/>
- Faucher P (2019) EU space surveillance and tracking framework a consortium of member states safeguarding European space infrastructure and orbital environment, presentation made by chairman, SMI conference, 2 Apr 2019
- Konacki M et al (2019) Optical, laser and processing capabilities of the new polish space situational awareness centre presentation done at AMOS conference, September 2019
- Malacz A, Konacki M, Malawski M (2018) Information of POLSA about polish accession to the EUSST consortium. Presentation at the April 2019 SSA conference, London
- Polish Government (2014) Act of 26 September 2014, Dz. U., 2014, poz. 1533
- Polish Government. Government Legislative Process. <https://legislacja.rcl.gov.pl/>
- Polish Government. Ministry of Development, Poland on Space 19+ <https://www.gov.pl/web/rozwoj/polska-na-space19%2D%2D-perspektywy-rozwoju-sektora-kosmicznego-na-najblizsze-trzy-lata>

Polish Space Agency-POLSA. <https://polsa.gov.pl/en/>

Polkowska M (2016) Polish Space Agency pursues task of developing country's space expertise. *Room Space J* 2(8):68–69

Polkowska M (2019) European challenges in SSA. Poland example, presentation at the Space Situational Awareness Workshop: perspectives on the future, directions for Korea, Seoul 24–25 Jan 2019

POLSA (2018) Polish Space Sector catalogue of selected entities. [https://polsa.gov.pl/images/polski\\_sektor\\_kosmiczny\\_katalog\\_pl\\_eng/PODGLAD\\_PAK-KATALOG\\_EN\\_small.pdf](https://polsa.gov.pl/images/polski_sektor_kosmiczny_katalog_pl_eng/PODGLAD_PAK-KATALOG_EN_small.pdf)

US Embassy and Consulate in Poland. <https://pl.usembassy.gov/ssa/>





Rajeswari Pillai Rajagopalan

## Contents

Introduction .....	500
Emerging Space Security Dynamics in Asia .....	500
Indicators of Conflict .....	502
Drivers of Space Conflict .....	507
What Can Be Done? .....	509
Conclusion .....	511
References .....	511

## Abstract

Asian countries are becoming increasingly active and more serious players in outer space. On the other hand, political and military competition in Asia are also impacting the Asian space efforts. The growing space competition is indicated by the rapid increase in counter-space capabilities such as anti-satellite (ASAT) missiles, electronic and cyber warfare capabilities as well as new efforts at creating specialized military agencies devoted to space utilization. There are three key drivers to space conflict in Asia – increasing use of space for military purposes; civilian use that could also lead to conflict because of congestion and competition; and investments in military technologies such as ASAT and missile defense. Existing global governance mechanisms are clearly inadequate to manage these challenges. While there are a number of different ideas including the Prevention of Arms Race in Outer Space (PAROS), political disagreements have so far prevented any progress. Unless the dangers inherent in this competition is recognised, the Asian space security efforts will only aggravate, which will further add to the challenges in developing global rules of the road. Key Asia-Pacific

R. P. Rajagopalan (✉)  
Nuclear and Space Policy Initiative, Observer Research Foundation, New Delhi, India  
e-mail: [rajeswarirajagopalan@gmail.com](mailto:rajeswarirajagopalan@gmail.com)

---

space players should make all efforts at developing legal measures, norms, Group of Governmental Experts (GGE), and codes of conduct.

---

## Introduction

Asia has been going through a strategic flux owing to the changing regional and global military balance. The growing trends of militarization and securitization of political and territorial issues mean there is a greater emphasis on hard power. This is beginning to play out in outer space affairs as well. The Asia-Pacific space landscape itself has been changing rapidly in recent times. Renewed anti-satellite (ASAT) tests starting with China's first successful test in January 2007 highlight a new phase in space security competition among the Asian great powers. Other spacefaring powers are re-examining their options, strategies, and capabilities, assigning a greater security role to their space programs. For instance, after the Chinese ASAT test, the USA undertook its own test in 2008. The Chinese test also sparked a new debate in India as to how it should defend its own satellites and whether it requires New Delhi to demonstrate its own ASAT capability. India's decision to finally have a demonstrated capability resulted in its first successful ASAT test in March 2019, following which India has conducted a tabletop war game called the "IndSpaceEx" with all the stakeholders including its scientific establishment and the military. Along with the capability development, India is also shaping its institutional architecture to develop the long-term strategies for space utilization and its integration into the armed forces.

These developments are merely a sign of the increasing insecurities on Earth and how outer space has become one more domain where the terrestrial politics are playing out (Pekkanen 2015). The growing indicators of space insecurity in the Asia-Pacific mean both use of space for terrestrial conflict and conflicts about use of space (Rajagopalan 2018a). In fact, the first could also lead to the second with greater integration of space in conventional conflicts leading to more insecurities and additional conflicts. But the impact of the changing global balance of power equations cannot be ignored. The changing power dynamics in both the Asia-Pacific and at the global level have had an effect on the region. Given that many of the rising powers are in Asia and some of them are challenging the prevailing geopolitical equilibrium, there is a big focus on acquiring hard power capabilities including in the outer space realm. While there are several internal and external factors pushing countries to respond in a more aggressive manner, the consequences are difficult to predict unless states are willing to adopt measures that will bring about a certain restraining effect on irresponsible behavior in outer space.

---

## Emerging Space Security Dynamics in Asia

The twentieth-century space competition played out between the USA and the Soviet Union, and the technology was restricted to a handful of countries, but the situation has changed dramatically. There are around 80 active space players

today, including also non-state, private sector commercial players. While the private sector participation in space is still a Western phenomenon, this is changing in the Asia-Pacific, including in countries such as China and India, which have traditionally not shared space with private sector. Japan has remained somewhat more open to private sector participation as compared to China and India. Entry of the private sector is important because they bring about innovation, thereby reducing the cost to access space. Access to outer space over the last couple of decades has become much more democratized with the spread of technology beyond the handful of countries who cherished the uses of space earlier. This however is not the problem. Given the significant utilities of outer space to a number of civil applications in changing the lives of ordinary people, more and more countries have pursued and will continue to develop space programs. The growing number of countries with space programs in Asia is also phenomenal. A look at the number of countries with independent launch capabilities in Asia – China, India, Iran, Israel, Japan, and North Korea – is a sign of the increasing interest and sophistication of space capabilities in Asia (Lele 2012). In addition, there are a growing number of emerging space players including Australia, Bangladesh, Indonesia, Iran, Israel, Malaysia, North Korea, Pakistan, Singapore, South Korea, the United Arab Emirates, and Vietnam (Moltz 2011).

Space security dynamics have become more complex partly due to the crowded and congested nature of space environment. A direct issue that arises from a crowded outer space realm is space traffic management and orbital debris that have implications for safe, secure, and sustainable use of outer space. But space is a dual-use asset, and many countries are beginning to use space for a variety of military and security applications. Radio-frequency interference, for instance, could be a result of the increasingly crowded nature of outer space, but there are also deliberate attempts to jam or otherwise impede radio signals (Powell et al. 2018; Weeden). Laser dazzling and blinding, or using cyber means to create temporary disruptions as well as denial of services, or to generate interference in command and control systems and logistics network, are worrisome (Attacking Satellites). These are a lot cheaper and more easily accessible, and there is plausible deniability with these technologies, making them more attractive as an option. In general, the increasing willingness to develop and possibly use counter-space capabilities is quite worrying, and the trend is particularly evident in the Asia-Pacific (Rajagopalan 2019a; Weeden and Samson 2019; Harrison et al. 2019). This is fueled by the fact that the Asia-Pacific houses some of the fastest growing economies, which in turn has aided higher military spending including in military space programs. All of this comes against the backdrop of an Asia that has already been bickering for several different reasons. Major power relations in Asia are one of the most contested ones, with these countries having gone into war with each other, and there are also unresolved sovereignty and border and territorial issues among these great powers. This historical background adds to the reality that three of the rising powers today are in Asia, which makes the political and security issues ever more challenging. Nevertheless, it is China's rise that has been the most spectacular and the most consequential in strategic terms.

In this regard, China's systematic rise as a major space power with consequences for regional and global security cannot be lost sight of (Columba Peoples 2013). China landed an unmanned mission on the near side of the Moon using its Chang'e 3 in December 2013, and in January 2019, its Chang'e 4 landed on the far side of the lunar surface, a feat not attempted by any other country until now (Jones 2019a). The next logical step for China in this regard would be to have a human lunar mission – Beijing has already stated its future Moon missions will take it closer to establishment of a possible research base on the Moon. China also plans to develop and operate its own version of the International Space Station (ISS) in low Earth orbit by 2024, by which time the current ISS will be wound up unless additional funding comes along to keep it running (Jones 2019b).

China's growing sophisticated space capabilities, in certain niche areas such as these, have driven the other two Asian space powers also to respond. India's recent attempt to soft land on the lunar surface faced a setback; nevertheless, it was a reflection of the budding Asian space competition. A successful mission would have made India the second Asian power to successfully carry out an unmanned lunar mission (Rajagopalan 2019b). Five years ago, India, in its first attempt, became the first Asian country to send an orbiter around the Mars, called the Mangalyaan (Rajagopalan 2013). India has more ambitions for its future including a mission to study the Sun, called the Aditya mission, a second mission to the Mars, and a Venus mission (For details, see Indian Space Research Organisation, <http://www.isro.gov.in>). But the emerging competition is not just in terms of attempting their own "firsts," but it is moving to the security domain as well, with more serious implications. India tested an ASAT weapon in March 2019, an effort to catch up with a capability that China had already demonstrated. After the Chinese ASAT test in January 2007, India had to possess its own deterrent capability to ensure its assets are protected (Rajagopalan 2011). Japan too has had impressive achievements such as a lunar orbiter mission in 2007 although it has followed more commercially viable projects such as the Hayabusa mission, the first time a spacecraft landed on an asteroid and brought back samples (Kodama and Hoshi 2019). Therefore, Asia will continue to witness both of these races playing out, and both of these are driven more by terrestrial power politics than any other factor (Rajagopalan 2019c). Asia will continue to have important achievements, but the tense geopolitics of the Asia-Pacific will further intensify the space security dynamics as well.

---

## Indicators of Conflict

Over the last decade, international tensions have risen in the Asia-Pacific region. This is partly the result of China's growth but also the consequence of China's behavior. China has found itself in conflict Space security:China's conflict with many countries in the region including with Japan, South Korea, Singapore, Vietnam, Australia, Malaysia, the Philippines, New Zealand, and India. Partly as a consequence of this, there is also strategic collaboration between Japan and Australia and between India and a number of countries in the region such as with Japan, South

Korea, Singapore, Vietnam, and Australia (Shaw 2019a). Again, as a consequence of this, there is also strengthening of relations between the USA and many of its partners in the region, which China in turn sees as a concern.

While some of the regional competition is giving way to more cooperative ventures, this is also driving states to develop more military space programs. Given that military operations are extremely net-centric ones, using shorter timeframes in a high-tech environment, integration of space has become absolutely critical. Operation Desert Storm and Iraqi Freedom demonstrated the “force-multiplier” nature of space, and since then major militaries have studied options to make their militaries exploit space as well. At the very least, more and more militaries are moving to develop space-based intelligence, surveillance, reconnaissance (ISR), positioning navigation and timing (PNT), satellite communications (SATCOM), information gathering, weather, environment, and terrain observation. Space has come to have a multiplier impact in terms of gaining greater sense of predictability of the operating environment for military missions on Earth, thereby reducing uncertainty and facilitating better command decisions. But these very same benefits become vulnerabilities as well – China, for example, has been investing in counter-space technologies because it sees space as USA’s Achilles’ heel because of the heavily networked US nature of US military operations.

One of the more direct manifestations of these growing tensions is the establishment of specialized space security institutions. Of course, the establishment of the US Space Force by President Trump received astonishing publicity by way of newspaper headlines. However, the reality is that the US effort is just the latest in a series of such actions and other major space powers have been setting up such forces as well. Even earlier, in 2011, Russia brought about certain institutional modernizations creating the Russian Aerospace Defence Forces which are meant for space security-related activities (Bodner 2018). Similarly, in 2015, China established the PLA Strategic Support Force (PLASSF) which saw the integration of the PLA space, cyber, and electronic warfare capabilities, which is considered a significant achievement considering the future of warfare that would see the interface between all these different capabilities (Kania 2018a; Davis 2019). India has its own plans to establish a Defence Space Agency. The establishment of these kinds of specialized space units has important implications for security in the Asia-Pacific. As space becomes more integrated and assumes more direct roles in conventional military operations, it can be expected that states would seek improved coordination of the military and security functions, which call for developing such specialized institutions.

A useful step will be to acknowledge that more and more countries are in the path to establishing such units. Without acknowledging this, it will be difficult to logically understand the rationale for such moves and the security conditions that are pushing countries to take such steps. As space gets further integrated into conventional military operations, the need to bring better coordination through institutions such as space force is real. While space force may sound like a fighting force, in reality it mostly seeks to achieve greater integration of functions and improved coordination levels among the several agencies involved. Nevertheless, it is

important to devote attention to these institutional changes and bureaucratic innovations because of their implications in the national security realm. Also, bringing to the open as much details as possible is important because in the absence of information, public debates become unnecessary alarmist and shrill, which is not helpful. Absence of information can also heighten the security dilemma which could further prompt more countries to go down this path. A few countries doing this and lack of information on why they are doing it could produce detrimental negative effects for all. The establishment of space-specific organizations such as “space commands” clearly does not mean we are about to enter a shooting war in space. Therefore, the usefulness of full appraisal of such institutions and their purposes are important in removing the alarmism that prevails and create more transparent and sensible debates on their realistic roles. Open debates of sorts on these issues can be an important transparency and confidence building measure (TCBM). With the prevailing great power politics, dialogue and transparency measures are important to stem the current trends where countries feel that the establishment of specialized units is a way to secure themselves. Especially since these new forces and commands are coming up primarily to aid greater coordination, openness and transparency, to a great extent, should be doable. These can go a long way in removing misperceptions and miscommunication among the major spacefaring nations. It is obvious that it is in the interests of every spacefaring nation to push forward certain norms and broad rules and regulations that guide the activities of the space forces and commands. But we are at the beginning of the process, and only a handful of states have so far established such specialized institutions. There is still time to regulate this space and not make it dangerous. Even until a decade ago, space was not implicated by terrestrial geopolitics, but that cannot unfortunately be said today. The growing insecurities among the Asian powers are visible including in outer space affairs.

As for the US Space Force, it is being established through the Space Policy Directive-4 of February 2019 that would facilitate the functioning of a joint-service combat command, envisaging greater integration with the air force, army, navy, marine corps, and other national security-related institutions (For more details, read Weeden 2019; Erwin 2019; Wang 2019). Specific satellite-based services that would need to see fuller coordination and collaboration among these agencies include GPS, satellite communications, missile warning, reconnaissance, and weather (Shaw 2019b). Meanwhile, a Space Command has been established, again, as a division within the Department of Defense on August 29, 2019, similar to the other 11 unified combatant commands that the USA has. The idea of a Space Command is not new – in fact, it existed in the past, established by President Reagan in 1985, but it was wound up in the early 2000s following the terrorist attacks on September 11, 2001. President Trump has, in essence, re-established the Command as a precursor to establishing a full-fledged Space Force as the sixth branch of the US military (Reichert 2019). The logic of the Space Command or a Space Force is very clear – to deal with competition from Russia and China. In a speech to the Pentagon, Vice President Mike Pence said, “Both China and Russia have been conducting highly sophisticated on-orbit activities that could enable them to manoeuvre their satellites

into close proximity of ours, posing unprecedented new dangers to our space systems. Both nations are also investing heavily in what are known as hypersonic missiles designed to fly up to five miles per second at such low altitudes that they could potentially evade detection by our missile-defense radars” (Remarks by Vice President Pence on the Future of the U.S. Military in Space 2018). He added that “China and Russia are also aggressively working to incorporate anti-satellite attacks into their warfighting doctrines. In 2015, China created a separate military enterprise to oversee and prioritize its warfighting capabilities in space. As their actions make clear, our adversaries have transformed space into a warfighting domain already. And the United States will not shrink from this challenge.” On the rationale for the Space Force, Pence said, “America will always seek peace in space as on the Earth, but history proves that peace only comes through strength and in the realm of outer space the United States Space Force will be that strength in the years ahead” (Remarks by Vice President Pence on the Future of the U.S. Military in Space 2018). While these statements are absolutely true, it is also a function of the worsening general security situation and also a result of the great power politics.

China has also consolidated its efforts at bringing greater integration of space functions. China’s establishment of the PLA Strategic Support Force (PLASSF) in 2015 became a significant institutional innovation as the PLASSF brought an effective amalgamation of space, cyber, electronic, and psychological warfare capabilities that were spread across other branches of the PLA and its former general departments (Costello and McReynolds 2018); for a detailed appreciation of the PLASSF and the role of outer space in PLA’s military operations see (Pollpeter et al. 2017). The Chinese efforts appear to be a Gold Nicholson moment for China aimed at bringing true integration of the PLA ground, naval, air forces, and the rocket wing, as per a *People’s Daily* report (Li 2016). In fact, a few months after the establishment of the PLASSF, Senior Colonel Yang Yujun, spokesperson of China’s Ministry of National Defense, said that the reorganization is “mainly to integrate the various types of support forces with strong strategic, basic and supportive functions. . . . The establishment of a strategic support force is conducive to optimizing the structure of military forces and improving comprehensive support capabilities. We will adhere to system integration, military-civilian integration, strengthen the construction of new combat forces, and strive to build a strong modern strategic support force. . . . It is conducive to the adjustment of functions and streamlining of institutional personnel by the military commission” (Ministry of Defense Spokesperson 2016). The Senior Colonel went on to add that “The Strategic Support Force is a new-type combat force for safeguarding national security. It is an important growth point of the military’s new combat capability. It is mainly formed for the functional integration of various types of support forces with strong strategic, foundational and supportive functions. The establishment of the Strategic Support Force is conducive for optimizing the military’s force structure and improving integrated support capabilities. [The PLA] will persist with system integration, military-civilian integration, the construction of new combat forces, and will strive to build a strong and modern strategic support force” (Ministry of Defense Spokesperson 2016). According to some of the sinologists tracking this institutional innovation, it will

be years before China can consolidate its reorganization process. They argue that “SSF is still in the process of consolidating, reorganizing and integrating the assorted capabilities and organizations that have fallen under its banner” (Ni and Gill 2019). Nevertheless, Adam Ni and Bates Gill have been able to put together a comprehensive picture of the SSF including the organizational structure, leadership, operational thinking, capabilities, and facilities. The two authors conclude that the PLASSF is “an important step in the PLA’s journey towards realizing integrated information operations and deploying an integrated strategic deterrent,” with a big focus in consolidating China’s military space and information warfare capabilities. Another analyst has gone on to say that the “future trajectory will be a critical bellwether of the PLA’s progress towards fulfilling its ambition of emerging as a ‘world-class’ military by mid-century” For a detailed Q&A on the PLASSF’s future directions including the doctrine, strategy, concept of operations, see (Kania 2018b)

Russia’s institutional innovation saw the birth of the Aerospace Defence Forces on December 1, 2011, combining the Air Defence and Space Forces. According to Russian reports, establishment of the Aerospace Force will be “the next logical step” with a goal to “organise military operations of multiservice force groupings in a common system of combat under a single leadership, in the new theatre of military operations” (Vekshin 2015). By way of providing the context, former Russian Air Force Commander, General Pyotr Deinekin, said, “Over the last decade the armed struggle all over the world has been actively shifting from near-Earth space to outer space,” and this has been the imperative to bring the air and space under a single command. In August 2015, Russia took the next step in further consolidating its conventional military forces by creating a new branch of service – the Aerospace Forces. According to Russian reports, these have been part of the efforts to modernize and integrate existing commands with a big focus on possible enemy air and space attacks against Moscow (McDermott 2015). In August 3, a few days after the establishment of the Aerospace Forces, Defense Minister Sergei Shoigu stated that the new organizational structure was “prompted by a shift in the center of gravity of the armed struggle toward the aerospace sphere” (See Ministry of Defense of the Russian Federation 2015). However, Russian scholars argue that this is not a mere combining of air and space assets under one single command, but President Putin’s August 1 decree makes the Aerospace Forces a full-fledged branch of the military, giving it equal importance like the army (McDermott 2015).

India over the last decade has begun to respond to changes in the neighborhood and beyond (Rajagopalan 2019d). The changing nature of warfare along with greater integration of space assets into conventional military operations has driven India to adapt with its own capacity building and institutional architecture. This has not come easy for India, a country that has traditionally maintained that space must be for peaceful purposes alone. At the same time, India cannot ignore the developments in its neighborhood and beyond – India’s concerns around space militarization and the early trends toward weaponization of space are real. But the new developments have made New Delhi approach space from a more nuanced perspective. For instance, India’s utilization of space assets for passive military applications such as surveillance and intelligence gathering is a case in point. India has increasingly



come to rely on space for its Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance (C4ISR) requirements. India is increasingly mindful of the fact that as militaries get dependent on space, there are also growing vulnerabilities with states developing capabilities to interfere with, disrupt, or damage these assets. The worsening trends in the overall security environment have further pushed India to get proactive in the last couple of years. India's ASAT in March 2019 is a consequence of this nuanced approach to space security. Further, India has gone on to establish the Defence Space Agency, a front runner to a full-fledged aerospace command (Lele 2019). These institutional structures are much required to bring greater synergy between the Department of Space, Ministry of Defence, and the military. India took the first step in this direction in 2008 with the establishment of the Integrated Space Cell within the Integrated Defence Headquarters, but the usefulness of the DSA will be to bring about better integration. While the DSA will be dealing with the strategy and policy questions affecting space utilization, India is now in the process of establishing a Defence Space Research Organisation (DSRO), along the lines of the Defence Research and Development Organisation (DRDO). But India must declare a space policy, which will be important as a tool for messaging to one's friends and foes alike. It can also bring about greater clarity in the domestic context which could also strengthen resource allocation.

---

## Drivers of Space Conflict

There are three broad drivers to space conflict – increasing use of space for military purposes; civilian use that could also lead to conflict because of congestion and competition; and investments in military technologies such as ASAT and missile defense. Each of the three drivers is playing out in the Asia-Pacific region given that the region also hosts new and rising powers.

In the Asia-Pacific region, there are not only a growing number of space players, but the region also hosts some of the most advanced military space programs. The geopolitical competition, for instance, between India and China and China and Japan, is becoming new imperatives for these countries to develop outer space capabilities beyond pure civil space programs. Given the growing military dependency on outer space, countries are also developing counter-space capabilities. China has grown by leaps and bounds in this area, since it has been looking at the USA as the primary competition. The rapidly advancing counter-space capabilities including electronic and cyber warfare capabilities are concerning to India, Japan, Australia, the USA, and other Asian powers. Even though no country has placed weapons in outer space, India and other spacefaring powers are concerned about China's anti-satellite capabilities that could function as an effective A2/AD especially during conflicts. It is quite evident that no country will want to place weapons in outer space, but using ground-based assets such as ASATs to destroy a satellite or deny satellite-based services is quite a real threat in Asia. But space security threats could also be a function of civil space activities. For instance, the crowded

and congested nature of outer space poses serious problems for most Asian nations, as they are still expanding their programs. Increasing space debris with the possibility of risking space assets is a serious issue. Along with the amount of space debris, a new problem is the proliferation of small satellites – mini, micro, and nano satellites – which makes the challenge of monitoring and detection of these satellites a bigger problem. In fact, there is a global trend toward breaking bigger satellite constellations into smaller ones, given that they are easier to launch and deploy, if interfered with or destroyed, for instance. At the same time, satellites have become a requirement for well-coordinated and synchronized tactical capability, integrating weapons systems, radars and sensors, and missiles, aerial capabilities, and logistical capabilities in vast geographical spaces like the Asia-Pacific. But complicating these is the dual-use nature of space and the entry of private sector in the military space arena. Launches carrying mixed payloads make it an even bigger challenge.

The growth and dispersal of military technologies has meant that many more countries are capable of investing in areas of technology that were previously limited to the superpowers. In addition, the spread of both missiles as well as increasing dependence on space for civilian and military purposes has meant that development of missile defenses and ASAT weapons has become more prevalent. A large number of countries now possess ballistic missiles – the spread of ballistic missile technology has meant a simultaneous pursuit of defenses against these missiles or at least the pursuit of such technologies. This search for a defense against missiles has accelerated in recent years. The increasing sophistication of surface-to-air missiles has led to adaption of such missiles also in antiballistic missile roles. Thus, the two prominent antiballistic missile systems, the American-built variants of the Patriot systems and the Soviet S-400 systems, have become increasingly popular. But countries like India (and Israel) have also pursued indigenous antiballistic missile systems because of the significant ballistic missile threats that both countries face. So, India has pursued Ballistic Missile Defence (BMD) at least since the mid-1990s, alternating between seeking to develop indigenous BMDs and acquiring it from abroad. India has shown interest in the Israeli Arrow and American BMD systems while also developing a domestic BMD program, built around the Prithvi missile system. Its capabilities remain unclear which is one reason why India has decided to acquire the S-400 system from Russia. China also has pursued BMD systems indigenously, but it is also buying the S-400s from Russia.

The increasing dependence on space-based systems as well as the growing capabilities of rocket engineering technology and more widely available sensor technology has meant increasing interest in ASAT systems. China demonstrated an ASAT capability in January 2007 which was possibly driven by China's pursuit of asymmetric capabilities against the far more capable American military forces. China's ASAT capabilities allow it to attack a vulnerable link in American military capability, but China's pursuit of ASATs, even if directed at the USA, clearly has implications for other powers such as Japan and India, countries that are also dependent on space for both civilian and military purposes. China's demonstration of its ASAT capability drove India immediately to begin its own ASAT program because it could not allow such a vulnerability given the competition between India

and China. Though neither country might actually deploy an ASAT system or use it in combat, demonstrating the capability was necessary for the purpose of deterrence. Following China's test in 2007, India also demonstrated its capability in early 2019.

---

## What Can Be Done?

The renewed emphasis on space security has brought the attention of all the key spacefaring powers to work toward some semblance of stability with regard to outer space activities. It is an entirely different issue that these countries are so far apart in identifying and agreeing upon major threats and the ways to address them. The existing treaties and other global instruments have regulated outer space activities to a great extent, but the re-emergence of counter-space as well as other new threats cannot be addressed effectively by the existing global mechanisms. There are gaps and ambiguities that should be addressed if one has to ensure safe, secure, and continued access to outer space (Rajagopalan 2018b). Given the worsening geopolitical trends, technologies with peaceful applications such as satellite inspection, refueling, and repair (on-orbit satellite servicing) or technologies to clean up space junk can be used for nefarious purposes. China has ground-based direct-ascent missiles that can physically destroy a satellite, jammers that can interfere, and lasers that can be used to dazzle or perhaps even blind imaging satellites and has also done a series of tests of on-orbit proximity and rendezvous operations, even though this is not indicative of explicit offensive capabilities. Similarly, Russia has a ground-based direct-ascent system known as Nudol, an airborne laser dazzler system known as the A-60 as well as GPS jammers. It has also engaged in a series of on-orbit proximity and rendezvous operations demonstrations, both in low Earth and geosynchronous orbits, and has shown high priority in integrating electronic warfare into military operations. The USA too has done multiple tests of technologies for close rendezvous operations; however, it does not have a declared direct-ascent ASAT program. Nevertheless, it possesses the capability to develop co-orbital ASATs should there be a decision to do so. It likely also has the capability to jam global navigation satellite service receivers such as GLONASS, BeiDou, and other regional navigation systems. Based on the growing inventory of counter-space capabilities among the key spacefaring nations, the Office of the US Director of National Intelligence, *2018 Worldwide Threat Assessment of the US Intelligence Community*, said, "We assess that, if a future conflict were to occur involving Russia or China, either country would justify attacks against US and allied satellites as necessary to offset any perceived US military advantage derived from military, civil or commercial space system." Adding to the complexities is the dual-use nature of space assets.

In the absence of successful multilateral efforts, states will be forced to rely on deterrence as a way of defending themselves. Deterrence could produce cascading effects because if one state relies on deterrence, others will be forced to as well and the net consequence will be negative for all. This could lead to increasing suspicions that will make cooperation difficult. There is still time left because the deterrence model has not yet become policy for any state regarding space, and therefore it is

possible to prevent it. One might add that it is necessary too, before states proceed down this path. Therefore, there is a small window of opportunity to halt the process of states pursuing deterrence as a state policy, but the bigger responsibility rests on the shoulders of all the major spacefaring powers to develop certain new rules of the road to address the more contemporary threats in outer space.

Yet the debates on the global governance aspects have not progressed much, and there are broadly two schools of thought. One school suggests that developing legal instruments are the way to address the gaps in the existing global mechanisms, whereas the second school argues that under the current international political climate, legal measures are unlikely and therefore they want to pursue political instruments such as a transparency and confidence building measures (TCBMs). But the EU Code of Conduct for Outer Space, a TCBM proposed a few years back, could not be adopted, even though the Code ran into problems mostly on process issues rather than on substantive issues on which there appeared to be significant agreement. Therefore, a point to be emphasized is that the process is as important as the substantive measures that are being developed. An inclusive process in developing a code or any TCBMs gives a large number of states a sense of ownership and responsibility to see that it becomes a success (Rajagopalan 2012). Accordingly, one might argue that even if the document is less than the ideal, it is more important to have a large number of state stakeholders to ensure its durability. However, in order to develop a large support base among the Asia-Pacific countries, it is important not only to have a critical number of states being party to it, but also the critical states need to be bought in. The lack of consensus among great powers has hampered the process of developing effective global measures. Within the Asia-Pacific again, there is no unity of approach to global rules of the road on space. For instance, Russia and China proposed a draft Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects (PPWT), first in 2008 and brought out a renewed text in 2014. But that has not gathered much momentum despite the fact that countries like India had generally preferred a legally binding mechanism (Listner and Rajagopalan 2014). In an effort to make some progress, there are those who have argued for a middle path: legally binding TCBMs. However, this has not generated much support either. Nevertheless, given the more tense space security environment today, there is a need to work on all possible tracks including legal measures and codes. The Conference on Disarmament (CD), where space security and arms control issues are debated, has been in a state of stalemate, and therefore the key spacefaring powers need to find innovative ways of approaching the global governance debates including the venue of such debates.

Irrespective of the outcome of the global governance front, there is a need for developing an effective Space Situational Awareness (SSA). Traditionally, the USA has maintained the largest SSA network with its radars and sensors, followed by Russia, which has a better coverage of the southern hemisphere. Europe has also developed certain capabilities in this regard. In the Asia-Pacific region, China, India, Australia, and Japan are developing SSA capabilities, and these need to be interlinked with other global networks. This is a relatively noncontroversial area

of cooperation that can instill greater confidence among major players in Asia who otherwise have difficult relations. But any player that wants to be a relevant stakeholder in this domain should develop these capabilities in order to have better awareness on how it impacts on their activities in outer space. The three essential activities – tracking of objects in space, monitoring space weather, and characterization of space objects – can go a long way in avoiding collisions ([Secure World Foundation](#)). SSA is useful also in addressing space weather – solar storms and explosions of charged particles that can damage satellites or even power grids on Earth.

---

## Conclusion

The challenges of space security are most pronounced in the Asia-Pacific. There is clearly no defense against ASATs. Moreover, there are no arms control measures or even TCBMs to address ASATs and other counter-space capabilities. Key Asia-Pacific space powers need to explore all ways to control these trends including legal measures, norms, Group of Governmental Experts (GGE), and codes of conduct. Given the continuing security threats and lack of progress on global governance, states need to invest in building better redundancy, hardening of space capabilities, and enhancing the security of backups.

---

## References

- Attacking satellites is increasingly attractive – and sangerous. *The Economist*, 18 July 2019. <https://www.economist.com/briefing/2019/07/18/attacking-satellites-is-increasingly-attractive-and-dangerous>
- Bodner M (2018) As trump pushes for separate space force, Russia moves fast the other way. *Defense News*, 21 June 2018. <https://www.defensenews.com/global/europe/2018/06/21/as-trump-pushes-for-separate-space-force-russia-moves-fast-the-other-way/>
- Columba Peoples (2013) Introduction: reading East Asia's space security dilemmas. *Space Policy* 29:95–98
- Costello J, McReynolds J (2018) China's strategic support force: a force for a new era. National Defense University, Washington, DC
- Davis M (2019) China's plans to dominate space. *The National Interest*, 15 April 2019. <https://nationalinterest.org/blog/buzz/chinas-plans-dominate-space-52562>
- Erwin S (2019) Air force nominee barrett calls for assertive US Posture on Space, says Space Force is a 'Key imperative'. *Space News*, 12 September 2019. <https://spacenews.com/air-force-nominee-barrett-calls-for-assertive-u-s-posture-on-space/>
- Harrison T, Johnson K, Roberts TG (2019) *Space Threat Assessment 2019*, Center for Security and International Studies, April 2019. [https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190404\\_SpaceThreatAssessment\\_interior.pdf](https://csis-prod.s3.amazonaws.com/s3fs-public/publication/190404_SpaceThreatAssessment_interior.pdf)
- Jones A (2019a) Chang'e-4 returns first images from lunar farside following historic landing. *Space News*, 3 January 2019. <https://spacenews.com/change-4-makes-historic-first-landing-on-the-far-side-of-the-moon/>
- Jones A (2019b) Chinese space station core module passes review but faces delays. *Space News*, 11 September 2019. <https://spacenews.com/chinese-space-station-core-module-passes-review-but-faces-delays/>

- Kania EB (2018a) China Has a 'Space Force.' What are its lessons for the pentagon? Defense One, 29 September 2018. <https://www.defenseone.com/ideas/2018/09/china-has-space-force-what-are-its-lessons-pentagon/151665/>
- Kania EB (2018b) China's strategic support force at 3. The Diplomat, 29 December 2018. <https://thediplomat.com/2018/12/chinas-strategic-support-force-at-3/>
- Kodama S, Hoshi M (2019) Asteroid landing a triumph for Japan's Space Industry. Nikkei Asian Review, 28 February 2019, <https://asia.nikkei.com/Business/Science/Asteroid-landing-a-triumph-for-japan-s-space-industry>
- Lele A (2012) An Asian space race? Space News, 21 November 2012. <https://spacenews.com/an-asian-space-race/>
- Lele A (2019) India needs its own space force. Space News, 28 May 2019. <https://spacenews.com/op-ed-india-needs-its-own-space-force/>
- Li J (2016) PLA's new support force to be hub of China's joint military operations. South China Morning Post, 24 January 2016. <https://www.scmp.com/news/china/diplomacy-defence/article/1904756/plas-new-support-force-be-hub-chinas-joint-military>
- Listner M, Rajagopalan RP (2014) The 2014 PPWT: a new draft but with the same and different problems. Space Review, 11 August 2014. <http://www.thespacereview.com/article/2575/1>
- McDermott R (2015) Russia reforms aerospace defense structures – again. Eurasia Daily Monit 12 (151), August 11, 2015. <https://jamestown.org/program/russia-reforms-aerospace-defense-structures-again/>
- Ministry of Defense of the Russian Federation (2015) Russian defense ministry army general sergey Shoygu holds regular teleconference. August 3, 2015 cited in Boston S, Massicot D The Russian way of warfare: a primer. RAND Corporation, 2017. [https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE231/RAND\\_PE231.pdf](https://www.rand.org/content/dam/rand/pubs/perspectives/PE200/PE231/RAND_PE231.pdf)
- Ministry of Defense spokesperson accepts media interview on issues related to Deepening national defense and military reform. 1 January 2016. [http://www.mod.gov.cn/info/2016-01/01/content\\_4637926.htm](http://www.mod.gov.cn/info/2016-01/01/content_4637926.htm)
- Moltz JC (2011) Asia's space race: national motivations, regional rivalries, and international risks. Columbia University Press, New York
- Ni A, Gill B (2019) The people's liberation army strategic support force: update 2019. China Brief 19(10), 29 May 2019. <https://jamestown.org/program/the-peoples-liberation-army-strategic-support-force-update-2019/>
- Pekkanen SM (2015) Asia's simmering rivalries are shifting to outer space, where anything goes. Forbes, 27 March 2015. <https://www.forbes.com/sites/saadiampekkannen/2015/03/27/asias-simmering-rivalries-are-shifting-to-outer-space-where-anything-goes/#405f1feb2090>
- Pollpeter KL, Chase ML, Heginbotham E (2017) The creation of the PLA strategic support force and its implications for Chinese Military Space Operations. Rand Corporation, Santa Monica
- Powell TD, Lubar DG, Jones KL (2018) Bracing for impact: terrestrial radio interference to satellite-based services. Center for Space Policy and Strategy, The Aerospace Corporation, January 2018. [https://aerospace.org/sites/default/files/2018-05/BracingForImpact\\_0.pdf](https://aerospace.org/sites/default/files/2018-05/BracingForImpact_0.pdf)
- Rajagopalan RP (2011) India's changing policy on space militarization: the impact of China's ASAT test. India Review 10(4):354–378
- Rajagopalan RP (2012) Writing the rules on space: why inclusion matters. Space News, 23 January 2012, <https://spacenews.com/writing-rules-space-why-inclusion-matters/>
- Rajagopalan RP (2013) India's race to mars goes way beyond science. The Wall Street Journal, 5 November 2013. <https://blogs.wsj.com/indiarealtime/2013/11/05/indias-race-to-mars-goes-way-beyond-science/>
- Rajagopalan RP (2018a) Asia in space: cooperation or conflict? Policy Forum, Asia & the Pacific Policy Society, Australian National University, 10 October 2018. <https://www.policyforum.net/asia-space-cooperation-conflict/>
- Rajagopalan RP (2018b) Space governance. Oxford Research Encyclopedias, Planetary Science Policy and Planning, Oxford University Press, August 2018. <https://oxfordre.com/planetaryscience/view/10.1093/acrefore/9780190647926.001.0001/acrefore-9780190647926-e-107>

- Rajagopalan RP (2019a) Electronic and cyber warfare in outer space. Space Dossier 3, United Nations Institute for Disarmament Research, May 2019. <http://www.unidir.org/files/publications/pdfs/electronic-and-cyber-warfare-in-outer-space-en-784.pdf>
- Rajagopalan RP (2019b) Chandrayaan 2 moon landing: the sign of a mature space mission. Hindustan Times, 6 September 2019. <https://www.hindustantimes.com/india-news/chandrayaan-2-moon-landing-the-sign-of-a-mature-space-mission/story-aTed8LJKpDVe3FenVeYiJl.html>
- Rajagopalan RP (2019c) China extends terrestrial rivalries into orbit with new space race. Nikkei Asian Review, 23 August 2019. <https://asia.nikkei.com/Opinion/China-extends-terrestrial-rivalries-into-orbit-with-new-space-race>
- Rajagopalan RP (2019d) India's strategy in space is changing. Here's why. World Economic Forum, 14 August 2019, <https://www.weforum.org/agenda/2019/08/indias-strategy-in-space-is-changing-heres-why/>
- Reichert C (2019) Trump formally establishes US space command. CNET, 29 August 2019. <https://www.cnet.com/news/trump-establishes-the-us-space-command/>
- Remarks by Vice President Pence on the Future of the U.S. Military in Space (2018) The Pentagon, 9 August 2018. <https://www.whitehouse.gov/briefings-statements/remarks-vice-president-pence-future-u-s-military-space/>
- Secure World Foundation. Space situational awareness. <https://swfound.org/media/205304/ssa-brochure-2015.pdf>
- Shaw N (2019a) India and Japan awaken to risks of superpower space race. Nikkei Asian Review, 8 January 2019. <https://asia.nikkei.com/Spotlight/Asia-Insight/India-and-Japan-awaken-to-risks-of-superpower-space-race>
- Shaw J (2019b) The US space force must be independent but not insular. Space News, 13 September 2019. <https://spacenews.com/op-ed-the-u-s-space-force-must-be-independent-but-not-insular/>
- Vekshin R (2015) Air force becomes an integrated new aerospace force. Russia Beyond, 1 September 2015. [https://www.rbth.com/economics/defence/2015/09/01/air-force-becomes-an-integrated-new-aerospace-force\\_393913](https://www.rbth.com/economics/defence/2015/09/01/air-force-becomes-an-integrated-new-aerospace-force_393913)
- Wang K (2019) US needs a space force to counter China. Asia Times, 24 April 2019. <https://www.asiatimes.com/2019/04/opinion/us-needs-space-force-to-counter-china/>
- Weeden B (2019) U.S. Space Command and Trump's Space Force can seem funny. But space threats are deadly serious. NBC News, 4 September 2019. <https://www.nbcnews.com/think/opinion/u-s-space-command-trump-s-space-force-can-seem-ncna1049251>
- Weeden B. Radio frequency spectrum, Interference and satellites fact sheet. Secure World Foundation. [https://swfound.org/media/108538/swf\\_rfi\\_fact\\_sheet\\_2013.pdf](https://swfound.org/media/108538/swf_rfi_fact_sheet_2013.pdf)
- Weeden B, Samson V (eds) (2019) Global counterspace capabilities: an open source assessment. Secure World Foundation, April 2019. [https://swfound.org/media/206408/swf\\_global\\_counterspace\\_april2019\\_web.pdf](https://swfound.org/media/206408/swf_global_counterspace_april2019_web.pdf)



# Chinese Space and Security Policy: An Overview

# 28

Zhuoyan Lu

## Contents

Introduction .....	516
Security in Space: Practices and Movements in China .....	517
Peaceful Uses and Exploration of Outer Space .....	517
Civil-Military Integration Policy in Space .....	518
Sustainability in Space: Endeavors from China in Promoting Space Stability and Preventing Conflicts .....	520
Space Debris Mitigation Measures in China .....	520
Radio Frequency Management Regime .....	521
Governance of Space: Space Policy-making in China .....	523
Conclusions .....	524
References .....	525

## Abstract

China's space policies have expanded in numerous areas and have generated enormous documents during the past decades. It is impossible to cover all topics within one chapter; however, during the past decade, particularly the last 5 years, some fundamental space policies have played a pivotal role in China's space security and sustainability development. Consequently, this chapter concentrates on these prominent movements and provides an overview of these policies.

---

Z. Lu (✉)  
International Space University (ISU), Strasbourg, France  
e-mail: [zhuoyan.lu@isunet.edu](mailto:zhuoyan.lu@isunet.edu)



## Introduction

China's journey towards space capability building began in 1956 with the establishment of the Aviation Industry Commission – to supervise and manage the Chinese aviation and space industry – in pursuit of national space development. China established its first launch site in 1958 and launched the first satellite in 1970. China tested the first unmanned spacecraft, Shenzhou-1, in 1999 and, later, in 2003 sent the first astronaut onboard spacecraft Shenzhou-5. China started the Moon exploration in 2007 by launching the Chang'e-1 satellite and deployed the first spacelab Tiangong-1 in 2011. At the same year, China completed the docking of Shenzhou-8 and Tiangong-1 and in 2013 Yutu rover landed on the Moon. In 2018, China released the first issue of Blue Book of China Aerospace Science and Technology Activities envisioning 40 launches in 2020, including the first Mars exploration mission and initiating the deployment of China's space station. Most recently, China successfully launched CZ-5 Y3 rocket, the heaviest launch vehicle ever, playing a significant role for the so-called super 2020 space plan.

China's aerospace industry has its origins on national defense. At the very beginning, aerospace technology was utilized for scientific exploration, technology development, military reconnaissance, and for other purposes that are mostly strategic to the State. However, as a space-faring nation, China is gradually taking more responsibilities for the international space governance and the maintenance of space for peaceful uses. This is reflected in the recently enacted 2015 National Security Law with the first ever reference to the peaceful uses and exploration of space.

Over the past 5 years, the Chinese space industry has been witnessing an increasing number of private space actors. This is in stark contrast with the situation prior to 2015, where China's aerospace industry was mainly dominated by two companies, the China Aerospace Science and Technology Corporation (CASC) and the China Aerospace Science and Industry Corporation (CASIC). This change in the space industry is closely related with the civil-military integration policy and its profound influence on China.

For international and national space development, not only does security play an essential role, but so does the sustainability aspect. The issue of space debris has raised international concerns, since it increases the chances for collisions in space and poses hazards to space objects in space as well as to the safety of property and life on the Earth. China has launched and deployed a considerable number of space objects and, therefore, space debris mitigation is one of the long-term policies and regulatory requirements. Nowadays, with the private space actors entering the space industry, some new measures and provisions are provided for space debris mitigation.

Radio frequency is another important element for consideration. To prevent harmful interference and to ensure access to and equal use of space, China has implemented a bunch of instruments for the management of radio frequency spectrum. This is critical for the sustainable development of space, as in the future the demand for frequency will increase while the availability of the resource will be a challenge for the government.

Space sector developments are supported and stimulated by national space policies, strategies, and regulatory frameworks. During the past decade, the space sector in China has experienced some significant moments, with some of them steering the space industry of the country towards a new page, some strengthening the responsibility of the country for peaceful exploration of space, and others reinforcing the duty of the country for space sustainability. This chapter will further illustrate these policies and regulatory making processes that cover space security and sustainability.

---

## Security in Space: Practices and Movements in China

### Peaceful Uses and Exploration of Outer Space

International space treaties comprise of five major instruments created in the 1960s and 1970s. The principle of exploration and use of outer space for “peaceful purposes” is ingrained in these treaties and followed by the international community. China is the State Party to four of the five treaties, namely, the Outer Space Treaty (1966), the Astronaut Agreement (1967), the Liability Convention (1971), and the Registration Convention (1974), yet China is not a State Party to the Moon Agreement (1979). The international space treaties have a binding effect upon State Parties and China as one of the State Parties to these treaties has to adhere to the rules and regulations set out in them.

The “Space White Paper” is the most important document for China’s space policy. Starting with the first issue of the Paper in 2000, the fundamental principles of the international space treaties are codified in China’s national space policy. In the Paper, it is stated that China promotes peaceful exploration and use of outer space, since outer space shall be the province of all mankind. The development objectives of China’s space industry are to:

- Explore outer space and expand the understanding of the universe and Earth
- Promote human civilization and social development for the benefit of all mankind by peaceful uses of outer space
- Meet the growing needs of economic construction, national security, scientific and technological development, and social progress
- Safeguard national interests and enhance comprehensive national strength

It also points out that the fundamental mission for China is to develop its economy and constantly promote the modernization process of the country. Therefore, the important role of space in safeguarding national interests and implementing national development strategies determine the purposes and principles of China’s space policy.

Although the principle of peaceful uses and exploration of outer space is constantly affirmed in China’s space policy, it is not enshrined in its national legislation.

In 2015, the National Security Law of the People's Republic of China was enacted and it clearly stipulates – for the first time ever in law – that China shall:

- Maintain peaceful exploration and use of outer space
- Enhance international cooperation
- Advance capabilities of scientific investigation and exploitation
- Protect the security of space activities, assets, and other interests

In fact, outer space does not fall under the jurisdiction of States' sovereignty. However, the particular legal status of the area has an influential impact on security, the latter shall be linked to the peaceful uses and exploration of outer space. This shall also be reflected in national legislation in order to further benefit international space activities.

### **Civil-Military Integration Policy in Space**

The space industry has long been dominated by States. In China, the turning point came with a decisive document in 2014 when the State Council released the "Guidance on Innovation of Investment and Financing Mechanisms in Key Fields to Encourage Private Investment." As such, private actors are stimulated to participate in the space industry and private capitals are encouraged to engage in this endeavor as well. Subsequently, 2015 marked the first year of China's commercial space with a "green light" to private entities, meaning less policy barriers in the upstream and downstream industry.

Further on, in 2015, the document on "Suggestions for the Thirteenth Five-year Plan for National Economic and Social Development" proposes the development of civil-military integration and requires the establishment of innovation in several fields including space. This accelerates the development of private space engagement in China. This policy is further detailed in the "Opinions on the Integrated Development of Economic and National Defense" whereby the civil-military integration is promoted to national strategic level. The latter allows for satellite data sharing, remote sensing resources integration, and dual-use navigation services. Later on, the "White Paper: China's Space Activities in 2016" reaffirms the policy and provides for management measures fostering the commercial space industry. A rationale behind the change is that the commercial space sector has been playing a considerably important role in the global space industry.

In order to further promote the civil-military integration, the "Central Civil-Military Integration Development Committee" was established in 2017, with two meetings held until now, one in June 2017 and another in March 2018. These meetings further set forth a central-local government system for civil-military integration: the central government provides top-level overall planning and the local government provides in-depth implementation measures and policies applicable to each administrative jurisdiction. Accordingly, more than 28 local governments

have released their local policies in promoting civil-military integration (Security RSS 2019). Most of the local policies include support of supplementary facilities, financial support for civil-military projects and programs investment, manufacturing, establishment, and the like. However, these policies vary from each other and apply only locally.

The “Civil-Military Integration” policy has not only been able to attract private capital in space sector but also has been successful in stimulating private space enterprises in China. For instance, in 2018 only, more than 70 private investors invested in over 30 space start-ups (EO Intelligence 2019). Statistics from Future Aerospace show that till the end of 2018 the number of commercial space companies registered are 141. Among them, 123 are private space enterprises, and 61 out of the 123 are founded in the recent 3 years (National Business Daily 2019). In addition, one private space company, founded in 2016, has been capable of three successful launches including two suborbital launches and one orbital launch within three years. The space business of private space enterprises covers a wide range of industry clusters, from launch to various satellite applications. Geographically they are grouped around Beijing, Xi’an, Shanghai, and other administrative jurisdictions, while among them Beijing accounts for over one half of the total.

In view of the successful outcome of the policy in promoting commercial space industry, the China National Space Administration (CNSA) continuously encourages and progressively promotes the commercial space industry in China by:

- (a) Fostering a friendly environment for commercial space enterprises
- (b) Improving the administrative mechanism and better serving the industry
- (c) Framing a policy and regulatory regime for the maintenance of a good order in space sector
- (d) Pushing the governing authorities to get actively engaged (CNSA 2019)

Apart from the impact on commercial space development, the civil-military integration policy also influences profoundly the scoping of regulation-making framework. Previously, both military authorities, the State Council and Ministries under the Council, were empowered to establish regulations and this mechanism has caused several conflicts during the past years. The drafting process of the Aviation Law and National Defense Mobilization Law are some examples. The ambiguity of regulatory scope, if not improved, will further deepen the gap. This situation led to the amendment of the Law that passed by the National People’s Congress (NPC) in 2015 (NPC 2015a, b). The amendment adds that national defense matters may be issued jointly by the State Council and the Central Military Commission, where previously the article stipulated that administrative regulations shall be issued solely by the State Council. Moreover, the civil-military integration policy further pushes relevant authorities to revisit the current regulatory framework and to abolish or update regulations that are out of date, like these two regulations: “Measures for Military Products Pricing” and “Measures for National Defense Research Project Pricing,” born at the 1990s, yet not applicable to the current commercial market.

## **Sustainability in Space: Endeavors from China in Promoting Space Stability and Preventing Conflicts**

### **Space Debris Mitigation Measures in China**

Space sustainability is a fundamental theme of China's national space policy provided that space environmental problems such as orbital congestion and the proliferation of space debris have become ever prominent. The Chinese government places great importance on it and steadily advances the work related to space debris mitigation, including the implementation of long march vehicles passivation, and undertaking post-mission disposal operations for many geostationary orbit satellites such as Fengyun meteorological satellite. The government of China is also actively engaged in international cooperation on space debris matters and holds a close relationship with the Inter-Agency Space Debris Coordination Committee (IADC).

In order to promote sustainable development of space activities, the Chinese government initiated a Space Debris Operation Plan for 2006–2020 with the following objectives:

- Generate earth- and space-based space debris monitoring network
- Design space debris protection program
- Prepare for space environmental protection

Space debris matters stated in the Plan are repeated in the 2016 White Paper "China's Space Activities," where one of the visions is related to space debris and it confirms that China will continuously improve the technology of space debris monitoring, early warning, and mitigation to safeguard spacecraft in orbit. It also aims to achieve technology breakthrough in spacecraft protection design.

As a follow-up to the policy, the Chinese government issued the "Aerospace Industry Standard of the People's Republic of China – Requirements for space debris Mitigation" in 2005. The latter aims to reduce the generation of space debris and bring down the risk of potential collisions and damages caused by space debris. In 2009, the government published the "Interim Measures for Space Debris Mitigation and Spacecraft Protection" and formulated more than 10 supporting regulations to push industries to follow space debris mitigation rules. The Interim Measures at the time of formulation referred to the Space Debris Mitigation Guidelines published by the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) and IADC.

In addition to the abovementioned efforts, space debris mitigation requirements are provided in regulations as well. As a State Party to the Registration Convention, China released the "Measures for Space Object Registration" in 2001. The document is the first regulatory instrument in China that governs space matters. Accordingly, all space objects, either launched in the territory of People's Republic of China or launched in a foreign country, yet China is a joint launching state, shall be registered with the State Administration of Science, Technology and Industry for National Defense (SASTIND). It is required that SASTIND shall maintain a space object registry containing necessary features of space objects. The registration regime has a

great advantage in space object identification and collision risk analysis, and it will further facilitate mitigation during the post-mission disposal in a long run.

Later on, China's "Interim Measures on the Administration of Licenses for Civil Space Launch Projects" came out in 2002. It requires civil space launch applicants to provide, alongside their applications, supplementary documents on measures to avoid the generation of space debris and prevent contamination of space environment. The same requirement is reiterated in the "Notice on Promoting the Progressive Development of Commercial Rocket Transportation" that was issued in 2019, and it also states that launch activities shall not impair national security and public interests.

The requirements of space debris mitigation measures are not only required for launch activities but also for satellite activities. This is based on the "Interim Measures for the Administration of Civil Satellite Projects" which requests entities involved in satellite industry to undertake their activities in accordance with the "Interim Measures for Space Debris Mitigation and Spacecraft Protection." The SASTIND supervises and manages the work of space debris mitigation and safety of civil spacecraft and launch vehicles, and also organizes the formulation of relevant measures and standards. However, the application scope of this instrument is limited to civil scientific and commercial satellites, and other engineering projects approved by the State Council or relevant Departments of the State that fully or partly use central financial funds.

In addition to regulations and requirements of space debris mitigation measures, in practice, the government of China also addresses scientific research for space debris. In 2016 the Ministry of Finance (MOF) together with the SASTIND issued the "Interim Measures for the Administration of Post-Subsidy for National Defense Science, Technology and Industry Research Projects" to further encourage innovation and developments in national defense science, technology, and industry. The implementation of the document will enable legal entities, research institutions, and universities that are registered in China to obtain funds from a central budget. It further forms 10 scientific fields applicable for this funding, with space debris scientific research being one of them.

In this manner, the government of China completes the national governance of space debris issues and with an emphasis on international cooperation for space debris mitigations, the country is trying to contribute to the capacity building of space sustainability and to comply with its international responsibilities. However, current circumstances of space debris and the condition of conjunction in space will remain and even get worse. The number of large constellations of small satellite keeps growing and thus space debris mitigation shall be maintained as a long-term strategy for the international community.

## **Radio Frequency Management Regime**

Radio spectrum is not only a limited resource but also a nonexhaustive one. On one hand, the continuous development of satellite technologies and applications brings an increasing demand on the use of radio spectrum since the resource is limited and it is therefore required to effectively manage and efficiently assign and allocate the

resource. On the other hand, the occupancy of a certain frequency and spectrum is not permanent, which makes it available for reuse after a period of time and consequently the supervision of efficient use and authorization of proper occupancy are critical for the resource management. In addition, supervision and authorization could enable the avoidance of harmful interference and maintain space sustainability for all.

From a policy and strategy perspective, the Ministry of Industry and Information Technology (MIIT) released the “National Radio Management Plan” (2016–2020). The Plan states the following working targets for the end of 2020:

- (a) Allocate radio spectrum in a more scientific manner
- (b) Manage radio activities more efficiently
- (c) Increasingly serve economic and social development, and national defense

In the Plan, it is reinforced that the government shall also work to improve the legal environment that governs radio spectrum activities. These include amending the Radio Regulation, cooperating with the judicial authority for the interpretation of article 288 of the Criminal Law of People’s Republic of China, and pushing the legislation of radio activities when appropriate.

China has developed a comprehensive regime governing the use of the radio-frequency spectrum, including both legislative and regulatory frameworks. In general, the legislations cover critical issues and activities with disruptive influences, while the regulations provide detailed rules accordingly. At legislative level, the “Property Law of the People’s Republic of China” was adopted by the National People’s Congress (NPC) in 2007 and it stipulates that the ownership of radio frequency spectrum resources shall be regulated by the State. For illegal use of the resource, the Criminal Law of the People’s Republic of China in 1997 covers the crime of disturbing the radio communication. In 2015, it was amended to include activities of setting up or using a radio station or a radio frequency without authorization, and in violation of State regulations, to interfere with the order of radio communication; such an activity causes severe consequences and is subject to penalties. Moreover, the Administrative License Law of the People’s Republic of China (2019 amendment) regulates the general establishment and implementation of the administrative license related to radio management and the Public Security Administrative Punishments Law of the People’s Republic of China (2012 amendment) stipulates that “the violation of relevant regulations and deliberately interfering with the operation of normal radio communication, or producing harmful interference to any normally operating radio stations, without eliminating the interference after receiving a warning from the authority, and causing severe consequences, shall be detained for punishments.”

The major regulations for radio spectrum management in China comprise of the Radio Regulation, the Radio Control Provisions, the Radio Spectrum Allocation Provisions, and other regulations, provisions, measures, and notices from the Ministries of the State Council. Currently there are more than 50 regulations and normative documents issued by the State Council, which are important supplements to the regulations on radio administration. For instance, despite the provision

provided in the Radio Regulation amendment of 2016 that the feasibility verification for the intended radio frequency shall be made during the planning phase of the satellite manufacturing. However, the regulation does not provide any further guidance in detail, such as how to carry out the verification and what shall be the feasibility verification elements in the process. In consequence, the “Measures for Feasibility Verification of Satellite Radio Frequency Occupancy” is introduced by MIIT in 2020 to bridge the regulatory gap. The “Measures” document explicitly specifies that the operator of the satellite is responsible for the feasibility verification process, the MIIT is in charge of supervision and guidance in the process, and the National Radio Spectrum Management Center provides technical support to MIIT.

Furthermore, remote sensing and space science satellites are one of the key areas of national civil space infrastructure. At the time of writing, China’s remote sensing and space science satellites have entered a new stage of development with a dramatic increase in the demand from the industry for radio frequency spectrum and satellite orbit resources. Reasonable and efficient utilization has therefore become essential for the government. The “Radio Frequency Utilization Plan for Remote Sensing and Space Science Satellites” (2019–2025) was created in 2019 with the aim to formulate plans for the use of satellite radio frequency and orbit resources, so as to guide relevant bodies to reasonably declare the use of satellite radio frequency and orbit resources. Such an instrument can be more responsive and effective for the needs and development of radio activities and has a profound influence in national radio spectrum management.

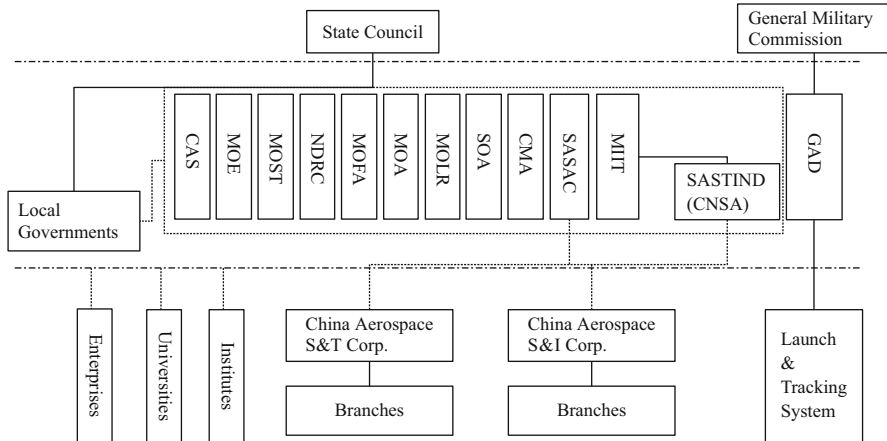
In China, the radio frequency matters are managed through a top down approach, central-local, separating civil from military uses. For the use of non-military radio system, the central management is under the following two authorities. One is the Ministry of Industry and Information Technology (MIIT) National Radio Administration Bureau (NRSA) and the Bureau is responsible for the preparation of radio spectrum plan, radio frequency allocation and assignment, supervision of radio station and radio interference, coordination of satellite orbits and the local-military radio management. The other one is the MIIT State Radio Monitoring Center (SRMC) who takes the responsibility of testing and certifying radio equipment, monitoring radio signals, positioning the interference radio and providing technical support for national radio management authorities and local radio management departments. For the management at the local government level, each local Radio Administration Office is responsible for the implementation of national radio policy, regulation, and provision, and is entitled to provide local radio management rules and licenses for radio stations, and to coordinate radio management matters within local jurisdiction.

---

## **Governance of Space: Space Policy-making in China**

The space policy-making in China involves various governmental departments from central government to local governments. The military system maintains a separate policy-making regime apart from the central-local governments. Depending on the level of the policy-making authority each policy may vary from each other. A space policy from the State Council has more persuasive authority than the policy from the





**Fig. 1** source from Handbook of Space Security 1<sup>st</sup> edition (2015) Chapter 24 Fig. 24.4

Ministry of the Council, while policies of different State Council Ministries are equivalent. For local government, a local regulation is prior to a local rule but is equal to a Ministry rule. In the previous edition of the Handbook (Schrogl et al. 2015), a detailed structure of space governance is provided and it shows how the policy-making mechanism is working in China.

In general, the State Council is the top policy-making body within the system, to which all the ministries and agencies are affiliated. Major ministries and agencies involving in space policy making include the State Administration of Science, Technology and Industry for National Defense (SASTIND), the former Commission for Science and Technology and Industry for National Defense, (COSTIND), the National Development and Reform Commission (NDRC), and the Ministry of Science and Technology (MOST). In particular, SASTIND is responsible for making the space industry policy, development plans, regulations, and standards, as well as for organization and coordination of major space programs. The NDRC – in charge of macroeconomic planning, operation, and adjusting – also gets involved in space industry policy making and commercialization of space technologies. The MOST is in charge of Science and Technology policy making and program management. Other governmental ministries and agencies involved in space policy making according to their functions and responsibilities are: the Ministry of Education (MOE), the Ministry of Foreign Affairs (MOFA), and the State-owned Assets Supervision and Administration Commission of the State Council (SASAC) (Schrogl et al. 2015) (Fig. 1).

## Conclusions

In the past decade, the space sector has been through several major changes. Private space industries have expanded almost across all the industry chain, from rocket manufacturing to satellite operations, and from ground infrastructures to service

providers. Hence, commercial space enterprises come in great numbers and attempt to position themselves in the market. These changes require national policies to regulate the activities of private actors. National policies attempt to create a dynamic and competitive environment for commercial space industries. The rapid development of the private space in the near future will lead to more favorable policies and governing measures. Accordingly, the role of government in space activities will gradually shift from the main rule-making and supervision authority to a more cooperative and open body.

Space is the frontier of science and technology and is an important area for national security. The international space order was formed in the 1960s and 1970s and the peaceful exploration and use of outer space remains fundamental for all nations and for all mankind. The reaffirmation of China's position in favor of peaceful uses and exploration of outer space represents the principles set forth in international treaties and indicate its responsibility as a space faring nation. In the new space era, the development of China's space industry will, as always, follow the established purposes mentioned in its policy and regulatory framework.

---

## References

- Agreement Governing the Activities of States on the Moon and Other Celestial Bodies (1979) RES34/68. [https://www.unoosa.org/pdf/gares/ARES\\_34\\_68E.pdf](https://www.unoosa.org/pdf/gares/ARES_34_68E.pdf). Accessed 30 Jan 2020
- Agreement on the Rescue of Astronauts, the Return of Astronauts and the Return of Objects Launched into Outer Space (1967) RES 2345 (XXII). [https://www.unoosa.org/pdf/gares/ARES\\_22\\_2345E.pdf](https://www.unoosa.org/pdf/gares/ARES_22_2345E.pdf). Accessed 30 Jan 2020
- CASC (2020) Blue book of China Aerospace Science and Technology Activities 2019 (in Chinese). <http://www.spacechina.com/n25/n2014789/n2014804/c2827360/content.html>. Accessed 30 Jan 2020
- CNSA (2019) China National Space Administration will support commercial space sector and promote the development of Commercial Space Industry (in Chinese). <http://www.cnsa.gov.cn/n6759533/c6806141/content.html>. Accessed 30 Jan 2020
- Convention on International Liability for Damage Caused by Space Objects (1971) RES 2777 (XXVI). [https://www.unoosa.org/pdf/gares/ARES\\_26\\_2777E.pdf](https://www.unoosa.org/pdf/gares/ARES_26_2777E.pdf). Accessed 30 Jan 2020
- Convention on Registration of Objects Launched into Outer Space (1974) RES 3235 (XXIX). [https://www.unoosa.org/pdf/gares/ARES\\_29\\_3235E.pdf](https://www.unoosa.org/pdf/gares/ARES_29_3235E.pdf). Accessed 30 Jan 2020
- CPC Central Committee, State Council, Central Military Commission (2016) Opinions on the Integrated Development of Economic and National Defense (in Chinese). [http://www.gov.cn/xinwen/2016-07/21/content\\_5093488.htm](http://www.gov.cn/xinwen/2016-07/21/content_5093488.htm). Accessed 30 Jan 2020
- EO Intelligence (2019) Research on space industry in China 2019 (in Chinese). <https://www.iyiou.com/intelligence/reportPreview?id=0&&did=663>. Accessed 30 Jan 2020
- MIIT (2016) National radio management plan (2016-2020) (in Chinese). <http://www.gov.cn/xinwen/2016-08/29/5103177/files/1d69478c03ae488fb1d97dff62d892c.pdf>. Accessed 30 Jan 2020
- MIIT (2018) Radio spectrum allocation provisions of the people's republic of China (in Chinese). <http://www.miit.gov.cn/n1146285/n1146352/n3054355/n3057735/n4699781/c7025032/content.html>. Accessed 30 Jan 2020
- MIIT (2020) Measures for feasibility verification of satellite radio frequency occupancy (in Chinese). <http://www.srrc.org.cn/article24153.aspx>. Accessed 30 Jan 2020
- MIIT, SASTIND (2019) Radio frequency utilization plan for remote sensing and space science satellites (2019-2025) (in Chinese). <http://www.miit.gov.cn/newweb/n1146300/n7121908/n7121930/c7309243/content.html>. Accessed 30 Jan 2020

- MOF, SASTIND (2016) Interim measures for the administration of post-subsidy for National Defense Science, Technology and Industry Research Projects (in Chinese). [http://www.mof.gov.cn/zhengwuxinxi/caizhengwengao/wg2016/wg201610/201703/t20170317\\_2559983.html](http://www.mof.gov.cn/zhengwuxinxi/caizhengwengao/wg2016/wg201610/201703/t20170317_2559983.html). Accessed 30 Jan 2020
- National Business Daily (2019) The development of commercial aerospace is in the ascendant with the help of new policies (in Chinese). <http://www.nbd.com.cn/articles/2019-06-11/1342005.html>. Accessed 30 Jan 2020
- NPC (2007) Property law of the people's republic of China (in Chinese). [http://www.gov.cn/flfg/2007-03/19/content\\_554452.htm](http://www.gov.cn/flfg/2007-03/19/content_554452.htm). Accessed 30 Jan 2020
- NPC (2015a) Legislation law of the people's republic of China (2015 Amendment) (in Chinese). [http://www.npc.gov.cn/zgrdw/npc/dbdhh/12\\_3/2015-03/18/content\\_1930713.htm](http://www.npc.gov.cn/zgrdw/npc/dbdhh/12_3/2015-03/18/content_1930713.htm). Accessed 30 Jan 2020
- NPC (2015b) National security law of the people's republic of China (in Chinese). [http://www.npc.gov.cn/wxzl/wxzl/2000-12/05/content\\_4581.htm](http://www.npc.gov.cn/wxzl/wxzl/2000-12/05/content_4581.htm). Accessed 30 Jan 2020
- SASTIND (2002) Interim measures on the administration of licenses for civil space launch projects (in Chinese). <http://www.mit.gov.cn/n1146295/n11652858/n7280902/c3554585/content.html>. Accessed 30 Jan 2020
- SASTIND (2016) Interim measures for the administration of civil satellite projects (in Chinese). <http://www.scio.gov.cn/xwfbh/xwfbh/wqfbh/35861/36552/xgzc36558/Document/1549898/1549898.htm>. Accessed 30 Jan 2020
- SASTIND, Central Military Commission Equipment Department (2019) Notice on promoting the progressive development of commercial rocket transportation (in Chinese). [http://www.gov.cn/xinwen/2019-06/17/content\\_5400951.htm](http://www.gov.cn/xinwen/2019-06/17/content_5400951.htm). Accessed 30 Jan 2020
- SASTIND, Measures for Space Object Registration (2001) (in Chinese). <http://www.scio.gov.cn/xwfbh/xwfbh/wqfbh/2013/20131216/xgzc29845/Document/1354170/1354170.htm>. Accessed 30 Jan 2020
- Schrogl K-U et al (eds) (2015) Handbook of space security: policies, applications and programs. Springer, New York
- Security RSS (2019) A collection of civil-military policies from local governments (in Chinese). <https://www.secrss.com/articles/9381>. Accessed 30 Jan 2020
- State Council (2014) Guidance on innovation of investment and financing mechanisms in key fields to encourage private investment (in Chinese). [http://www.gov.cn/zhengce/content/2014-11/26/content\\_9260.htm](http://www.gov.cn/zhengce/content/2014-11/26/content_9260.htm). Accessed 30 Jan 2020
- State Council, Central Military Commission (2010) Radio control provisions of the people's republic of China (in Chinese). [http://www.gov.cn/zwgk/2010-09/06/content\\_1696833.htm](http://www.gov.cn/zwgk/2010-09/06/content_1696833.htm). Accessed 30 Jan 2020
- State Council, Central Military Commission (2016) Radio regulation of the people's republic of China (in Chinese). [http://www.gov.cn/zhengce/content/2016-11/25/content\\_5137687.htm](http://www.gov.cn/zhengce/content/2016-11/25/content_5137687.htm). Accessed 30 Jan 2020
- State Council Information Office (2006) White Paper: China's space activities in 2006 (in Chinese). <http://www.scio.gov.cn/zfbps/ndhf/2006/Document/307876/307876.htm>. Accessed 30 Jan 2020
- State Council Information Office (2016) White Paper: China's space activities in 2016 (in Chinese). <http://www.scio.gov.cn/vz/Document/1537090/1537090.htm>. Accessed 30 Jan 2020
- Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (1966) RES 2222 (XXI). [https://www.unoosa.org/pdf/gares/ARES\\_21\\_2222E.pdf](https://www.unoosa.org/pdf/gares/ARES_21_2222E.pdf). Accessed 30 Jan 2020



# Chinese Concepts of Space Security: Under the New Circumstances

# 29

Dean Cheng

## Contents

Introduction .....	528
Evolution of Chinese Thinking About Military Space .....	528
Space and Local Wars Under Modern, High-Technology Conditions .....	528
Space and Informationized Local Wars .....	530
Chinese Space Capabilities: A Brief Review .....	531
Chinese Concepts of Military Space Operations .....	533
Space Dominance and Information Dominance .....	536
Mission Areas Associated with Space Operations .....	537
Space Deterrence (kongjian weishe; 空间威慑) .....	538
Space Blockade (kongjian fengsuo zuozhan; 空间封锁作战) .....	540
Space Strike Operations (kongjian tuji zuozhan; 空间突击作战) .....	540
Defensive Space Operations (kongjian fangyu zuozhan; 空间防御作战) .....	542
Space Information Support Operations (kongjian xinxi zhiyuan zuozhan; 空间信息支援作战) .....	543
Space and Information Dominance “Under the New Circumstances” .....	544
Creation of the PLA Strategic Support Force (PLASSF) .....	546
Civil-Military Integration of Space Industrial Capabilities .....	547
Conclusions .....	549
References .....	551

## Abstract

Chinese thinking about the relationship of space to national security has been evolving over the past several decades, as part of a broader ongoing assessment of the role of information in future warfare. As the People’s Liberation Army has accorded growing importance to information and communications technologies, the centrality of space dominance has grown as well.

---

D. Cheng (✉)  
The Heritage Foundation, Washington, DC, USA  
e-mail: [dean.cheng@heritage.org](mailto:dean.cheng@heritage.org); [deanbcheng@gmail.com](mailto:deanbcheng@gmail.com)

## Introduction

Since Xi Jinping came to power in 2012, he has been propounding the “China Dream” involving the “great revival of the Chinese people.” A central part of this “China dream” is a strong military. This effort to modernize and strengthen the Chinese People’s Liberation Army (PLA) occurs within a broader context of an evolving Chinese view of future warfare. Assessing other peoples’ wars, the Chinese concluded that future wars would include space warfare as an integral part of operations. This has not been so much because of the importance of space systems as such, as their growing role in providing the information support necessary for the successful conduct of future local wars, which are characterized as occurring under “informationized conditions.”

Indeed, PLA assessments of American and Russian military operations concluded that space-based information played an outsize role in the conflicts of the 1990s, and therefore, in the event of a conflict with the PRC, it must strive to deny an adversary the ability to use space freely. Thus, space warfare and information warfare have long been intimately linked in the Chinese mind.

---

## Evolution of Chinese Thinking About Military Space

While China’s space program dates from the 1956 founding of the Fifth Academy of the Ministry of Defense, it is not clear how the PLA thought about space, if at all, in the early years. This is likely due, in part, to the skepticism Mao exhibited toward military professionalism. For many years, it was more important for the PLA to be “red,” i.e., ideologically reliable, than “expert,” proficient in the military arts.

This was compounded by the limited space capabilities available to the PLA. China only launched its first satellite in 1970. In the ensuing decades, it only orbited a handful of communications and reconnaissance satellites. Chinese military planners therefore did not necessarily have a full understanding of the potential capabilities space provided. Moreover, space was seen as more a political gesture than a vital part of the economic or military arena and therefore was a lower priority, especially for Deng Xiaoping. After he succeeded Mao, Deng made it clear that the Chinese space program needed to focus less on gaining prestige and headlines and instead “concentrate on urgently needed and practical applied satellites” (Li 1999).

## Space and Local Wars Under Modern, High-Technology Conditions

The coalition performance against Iraq in 1990–1991 during Operation Desert Shield/Desert Storm served as a wake-up call for the PLA. This included highlighting the importance of space as one of the key high-technology areas that would influence the course of future wars, since it is a key enabler of joint operations.

As envisioned by the PLA, joint operations would involve multiple services operating together across significant distances. The Gulf War, for example, sprawled across some 140 million square kilometers and included forces ranging from armored units to aircraft carriers and long-range bombers (Wang and Zhang 2000, p. 400). The ability to coordinate such diverse forces spread across a variety of domains would therefore require not only extensive communications but also precise navigation and positioning information, both for units and for the growing plethora of precision munitions. Space-based platforms would play an essential role in the command and control of joint operations.

In this light, space capabilities were recognized as playing an essential role in any effort to wage a “local war under modern, high-tech conditions.” According to PLA estimates, the 70 satellites that were ultimately brought to bear against Iraq provided the United States with 90% of its strategic intelligence and carried 70% of all transmitted data for coalition forces (Gao 2001, p. 54). Indeed, these assets were the first to be employed, since they were essential for the success of all subsequent campaign activities. As one Chinese analysis observed, “Before the troops and horses move, the satellites are already moving” (Gao 2005).

The growing importance of space was not immediately recognized, however. In the 1997 *PLA Military Encyclopedia*, the discussion for “space warfare (*tianzhan*; 天战)” explicitly states that space is *not* a decisive battlefield – the key to wartime victory would remain in the traditional land, sea, and air realms. “It is impossible for it [space warfare] to be of decisive effect. The key determinant of victory and defeat in war remains the nature of the conflict and the human factor” (PLA Encyclopedia Committee 1997, p. 602). Space was seen as a supporting, not a leading, player.

By 2002, this view had evolved. In that year’s supplement to the *PLA Encyclopedia*, a very different assessment is made of the importance of space. In a discussion of the “space battlefield (*taikong zhanchang*, 太空战场),” the chapter concludes with the observation that the impact of the space battlefield on land, sea, and air battlefields will become ever greater and the space battlefield “will be a major component of future conflict” (PLA Encyclopedia Committee 2002, p. 455). It is clear that, in the intervening 5 years, the perception of space had changed and was now seen as a substantially more important arena for military operations.

This progression may have been partly due to the intervening NATO conflict in the Balkans. The ability to defeat Belgrade through airpower, seemingly on its own, clearly caught Beijing’s attention. In their analyses of that conflict, the Chinese accorded great prominence to the role of space power. NATO forces are assessed to have employed some 86 satellites (Zhang et al. 2005). Another Chinese analysis concluded that NATO space systems provided 70% of battlefield communications, 80% of battlefield surveillance and reconnaissance, and 100% of meteorological data and did so through all weather conditions, 24 h a day (Jiang 2013, p. 65). These provided a dense, continuous flow of real-time data, allowing the NATO forces to establish precise locations for Serbia’s main military targets for sustained, coordinated strikes, with 98% of the precision-guided munitions employing space-based information (Liu and Wang 2008, p. 44; Jiang 2013, p. 65). Thus, airpower could achieve its goals only because it was supported by substantial space power.

Given the importance of such support from space systems, victory in future “local wars under modern, high-technology conditions” was already recognized as requiring not only one’s own unfettered access to space but also the denial of the same ability to the adversary. The focus, however, was not so much on space systems as the information gathered by transmitted via those systems.

By preventing the enemy from obtaining the amount of information they required, it would be far more difficult for them to coordinate their forces and operations. As important, by preventing them from operating in the manner to which they were accustomed (and had trained), they would be far less efficient and flexible and therefore more vulnerable to Chinese actions. In effect, by degrading adversary space capabilities, the enemy would suffer from a slower OODA (observe-orient-decide-act) loop. Space information support was therefore not only a vital part of joint operations but would increasingly be complemented by offensive space operations (which somewhat aligns with Western concepts of counter-space operations).

## Space and Informationized Local Wars

This shift may also have been a reflection of the ongoing development of Chinese concepts of future warfare. As part of the PLA’s “new historic missions,” Hu Jintao in 2004 made clear that the PLA must secure China’s interests in outer space, as well as the electromagnetic spectrum (Hu 2004). (For further discussion of the “new historic missions,” see (Hartnett 2008).) The incorporation of the space domain into the specific range of PLA responsibilities reflected the steadily growing emphasis placed upon establishing space dominance as part of the larger effort to secure information dominance.

Indeed, as the PLA shifted from preparing to fight “local wars under modern, high-technology conditions” to fighting “local wars under informationized conditions” and then to “informationized local wars,” space has been increasingly seen as part of those “informationized conditions.” As PLA writings noted, “informationized conditions” do not simply refer to computers and cyberwarfare. Instead, it involves the acquisition, transmission, and exploitation of all forms of information. Space plays a central role in all these tasks. In the 2006 edition of *The Science of Campaigns*, it is specifically stated that “the space domain daily is becoming a vital battle-space.... Space has already become the new strategic high ground” (Zhang 2006, p. 87).

This is exemplified in that volume’s revised version of “campaign basic guiding concept.” This concept of “integrated operations, precision strikes to control the enemy (*zhengti zuozhan, jingda zhidi*; 整体作战, 精打制敌)” has even more need for information support from space-based assets than the previous version of “integrated operations, key point strikes.” For example, precision strikes involve the use of precision munitions to attack vital targets. The goal is not only destroying key targets but also precisely controlling the course and intensity of a conflict (Zhang 2006, p. 81). It also entails disrupting the ability of the enemy’s systems (and

systems of systems) to function normally. The focus is on disruption leading to paralysis, not just destruction of the adversary's weapons or forces (Wang and Zhang 2009, pp. 202–203). Information from space systems facilitates the conduct of such precision operations. “Establishing space dominance, establishing information dominance, and establishing air dominance in a conflict will have influential effects” (Zhang 2006, p. 83).

Similarly, in the 2013 edition of *The Science of Military Strategy*, space is deemed the “high ground in wars under informationized conditions,” tied to the struggles in network space and the electromagnetic spectrum as key future battlegrounds (Academy of Military Science Military Strategy Research Office 2013, pp. 146–147). In the Chinese conception, space is important for the advantage it confers with regard to the ability to collect, transmit, and exploit information, rather than for its own sake. As other Chinese analysts conclude, “space operations will be a core means of establishing information advantage” (Yuan 2008, p. 324).

---

## Chinese Space Capabilities: A Brief Review

China's overall space capabilities have expanded significantly during the past two decades. Indeed, its growth during this period is in sharp contrast to its first 20 years. From 1956 to 1976, China enjoyed only very limited advances in its space capabilities, due to a lack of financial, technological, and trained human resources, as well as repeated political upheavals that disrupted research efforts. Even after orbiting its first satellite, in 1970, space development remained limited, with only a handful of satellites orbited before Mao died in 1976.

Deng Xiaoping initially did little to promote space development for either the military or civilian sectors. For his first several years in power, rather than committing further resources toward space, Deng focused on developing the civilian economy, forcing the space industrial sector to fend for itself through conversion to products with civilian demand.

Support for China's overall space program did not improve until 1986, when Deng, at the urging of a number of top Chinese scientists, authorized Plan 863, formally termed the National High-Technology Research and Development Plan (*guojia gao jishu yanjiu fazhan jihua*; 国家高技术研究发展计划). (Material drawn from *Guojia Gao Jishu Yanjiu Fazhan Jihua 863*, in FBIS-CHI (July 21, 2000). For further discussion of the creation of Plan 863, see (Feigenbaum 2003, pp. 141–143.) Plan 863, which remains an ongoing effort, was seen as providing the scientific and technological research foundations essential for a modernizing economy. Aerospace, along with information technology, and later telecommunications were seen as key areas of high technology, justifying substantial, sustained resource investment.

In the 1990s, with renewed support from senior leaders, China's space program benefited from expanded investment and intensified high-level support. Under Jiang Zemin (1992–2002), China deployed both low-Earth orbit and geosynchronous weather satellites (the *Fengyun* series) and improved geosynchronous



communications satellites (the *Dongfanghong-3* series), as well as recoverable satellites with varying payloads (the *Fanhui Shi Weixing* series).

Chinese Earth observation capabilities also improved during this period. In cooperation with Brazil, China in 1999 deployed the China–Brazil Earth Resources Satellite (CBERS), its first electro-optical imaging satellite capable of beaming its pictures directly down to Earth. China subsequently launched several similar satellites with no Brazilian involvement; these are known as the *Ziyuan* series, to distinguish them from the CBERS satellites.

In 2000, China became only the third country to deploy a navigational satellite system, launching two *Beidou* regional navigation satellites into geosynchronous orbit. This system also has a communications function, which was employed during the 2008 Sichuan earthquake (Lu 2008).

Jiang Zemin’s successor, Hu Jintao, maintained support for China’s space program. During his two terms, China deployed a variety of new satellite systems, including remote sensing satellites (the *Yaogan* series), microsattellites such as the *Shijian* series, as well as improved versions of the *Fengyun* and *Ziyuan* satellites. Under Hu, China also orbited several manned spacecraft (the *Shenzhou* program), as well as initiated a lunar exploration program, launching the *Chang’e-1* and -2 lunar probes.

Chinese leader Xi Jinping has placed even greater emphasis upon the development of China’s aerospace capabilities. He has repeatedly stated that China must become a “major aerospace power (*hangtian qiangguo*; 航天强国).” Indeed, the Chinese official news agency Xinhua at one point released a series of quotations from Xi from 2013 through 2019 on this very issue, under the title “Xi Jinping Repeatedly Supports Building a Major Space Power” (Xi Jinping 2019).

Chinese space capabilities have steadily improved under Xi. China inaugurated its *Gaofen* series of high-resolution Earth observation satellites in 2013. The second Chinese space lab, *Tiangong-2*, was launched in 2016, reflecting China’s continued interest in manned space missions. China’s *Chang’e-3* mission deployed the lunar rover *Yutu* (Jade Rabbit) in 2013, the first mission to land on the Moon since Apollo 17. In 2018, China landed *Chang’e-4*, the first probe to ever explore the lunar far side and polar regions.

In keeping with Deng Xiaoping’s admonition that China’s space program must serve the broader goal of national economic development, many of China’s satellites are dual-purpose, supporting urban planners and agricultural programs as well as the military. For many of its satellite programs, including Earth observation satellites, position and navigation systems, and weather satellites, the focus has been more on providing suitable information to support Chinese economic development objectives than necessarily producing cutting-edge capability.

This has also been a two-way street. The Chinese space industrial complex has benefited from the steady investment of resources to develop space capabilities. Much of China’s space technology has been indigenously developed; Chinese satellites, launch vehicles, and ground support equipment are largely domestically produced. Two major aerospace conglomerates, the China Aerospace Science and Technology Corporation (CASC) and the China Aerospace Science and Industry

Corporation (CASIC), manufacture the full range of space systems, including launch vehicles, satellites, and ground equipment, and the associated sub-systems and support items.

Similarly, there is recognition that a strong national space infrastructure will benefit the military as well. Military space systems, by their exquisite nature and extreme capabilities, are expensive and therefore necessarily limited in number. Civilian space assets are likely to be more robust in numbers and are also in many cases developing faster than their military counterparts. Consequently, Chinese analysts conclude that a comprehensive set of civilian space systems can usefully augment military space forces, at least in terms of space information support and space monitoring (Ma 2013, p. 220).

---

## Chinese Concepts of Military Space Operations

China's space program is not solely devoted to civilian use, however. It also provides the PLA with key pieces of information, deemed essential for "informationized local wars." Moreover, the military plays an outsize role in Chinese space activities, as the PLA runs China's space facilities. (Up until December 31, 2015, the PLA was managed by several General Departments which oversee all the armed forces, including all the services. These were the General Staff Department (GSD), the General Political Department (GPD), the General Logistics Department (GLD), and since 1998 the General Armaments Department (GAD). These Departments comprised the membership of the Central Military Commission (CMC) until 2004, when the PLA Navy, PLA Air Force, and Second Artillery were added to the CMC.)

Under Hu Jintao, the PLA began to demonstrate overt space combat capabilities. The PLA tested its direct ascent, kinetic kill anti-satellite (ASAT) system in January 2007. Launched from Xichang Satellite Launch Center, the Chinese ASAT destroyed a defunct Fengyun-1C weather satellite in low orbit. In the process, China also generated a massive amount of space debris (David 2007). Almost precisely 3 years later, in January 2010, China engaged in what was termed an anti-missile test, involving "two geographically separated missile launch events with an exo-atmospheric collision also being observed by space-based sensors," according to the US Department of Defense (China: Missile 2010). This test also helped Chinese scientists improve their ASAT system. And in August 2010, two Chinese microsatellites were deliberately maneuvered into close proximity and apparently "bumped" each other (Matthews 2010).

This effort at developing anti-satellite systems has been sustained under Xi Jinping. In May 2013, the Chinese conducted another anti-satellite test. This weapon, however, is assessed as demonstrating an ability to threaten targets as far as the geosynchronous belt, over 26,000 miles away (Weeden 2014). This is the first time that any nation has tested a weapon explicitly intended to hold satellites in that orbit at risk. Described by one senior US military officer as the "most valuable orbit," the geosynchronous region is populated by not only large numbers of communications satellites but also strategic early warning satellites as well as weather satellites

(Gruss 2015). The ability to destroy such satellites would be a major step toward establishing information dominance.

As with other Chinese military activities, the PLA's approach to space operates within the context of "guiding thoughts." The "guiding thoughts" for space are "active defense, all-aspects unified, key point is dominating space (*jiji fangyu, quanwei yiti, zhongdian zhitian*; 积极防御, 全维一体, 重点制天)" (Jiang 2013, p. 40). Each of these phrases embodies a number of essential concepts.

*Active defense* is integral to all Chinese military strategies and, as noted earlier, is not limited to space-related operations. While assuming the strategic defensive, the PLA concept of "active defense" emphasizes the importance of seizing the initiative at the tactical and operational level. In the context of space operations, "active defense" again assumes a more strategically defensive stance, although one which nonetheless seeks to deter aggression and maintain national security and interests. Chinese military writings assume that in space, as terrestrially, the Chinese would not be the party responsible for precipitating a war. At the same time, however, the "active defense" expects the PLA to undertake space combat preparations so as to be able to seize the initiative in space-related operations. In particular, it presumes "offensive actions at the campaign and tactical level to secure strategically defensive goals" (Jiang 2013, p. 40).

"*All aspects unified*" refers to the need to unify thinking about a number of different aspects of space operations. In the first place, it entails viewing space as a holistic environment, encompassing not just the satellites that are in orbit but also the terrestrial mission control; launch; and tracking, telemetry, and control (TT&C) facilities that allow those satellites to operate, as well as the data links that bind the entire structure together. In striving to achieve space dominance, the Chinese envision attacking and defending all three components. The destruction of mission control facilities, the jamming of TT&C links, or the entry of instructions that turn off the satellite at key moments can be every bit as effective as launching an ASAT against a given satellite.

"All aspects unified" also requires viewing the various domains of military activity, including not only outer space but land, sea, air, and the electromagnetic spectrum (e.g., cyber and electronic warfare operations), in a joint fashion, with operations in each domain contributing to, and requiring support from, the other domains. Since space operations are an integral part of joint operations and especially information operations, it is essential to adopt a joint perspective, not only to forge an organic, integrated whole but also so that each component force supplements the others (Li 2012, p. 98). Space operations support terrestrial operations, while land, sea, air, and computer network operations can help achieve space superiority. All of these operations, in turn, are ultimately aimed at achieving predetermined political ends.

Similarly, "all aspects unified" requires seeing all the various wartime activities, including offensive and defensive operations, provision of information support and fire support, and hard- and soft-kill methods, in an integrated or unified fashion, rather than as discrete phases, tasks, or methods. Thus, proper conduct of space operations should involve the application of "soft-kill" methods such as dazzling or

jamming, in coordination with “hard-kill” methods such as direct ascent kinetic kill vehicles. Space operations should be coordinated with terrestrial operations, not only for the provision of meteorological, positioning and navigation, and communications information from space systems but also for air, land, and sea attacks on an enemy’s space launch and mission support facilities. As with cross-domain operations, the various methods and activities should be seen holistically, all contributing to the goal of establishing space dominance, in support of establishing information dominance, while also serving the larger, strategic ends of the overall campaign.

To this end, command and control of space operations plays a central role. Not only must the various space activities, including offensive and defensive operations, be closely controlled, but competing demands for reconnaissance and early warning, communications, navigation, and various other space information support assets must also be managed. This encompasses not only military space assets but civilian and commercial systems as well. Space operations must therefore be integrated into the larger joint campaign plans to help achieve terrestrial objectives. Command and control of space operations must reconcile space-related requirements, timing, and structure with those of the overarching joint campaign (Jiang 2013, p. 43). This integrated command and control network, capable of drawing upon military, civilian, and commercial resources, is a vital means of achieving “all aspects unified.”

“*Key point is establishing space dominance*” in part builds upon the PLA’s emphasis on striking the enemy’s “key points (*zhongda yao hai*; 重打要害),” especially those nodes within the enemy’s “combat system-of-systems (*zuozhan tixi*; 作战体系).” As a “key point” is to establish space dominance, the PLA commander is expected to concentrate his best forces and capabilities to precisely strike key targets with a combination of hard- and soft-kill weapons, with the goal of paralyzing the adversary.

The massive advances in information technology have meant that forces and weapons are now much more networked across the land, sea, air, space, and electromagnetic/cyber domains. While this has significantly advanced combat effectiveness by creating synergies across various forces, it has also introduced a new set of vulnerabilities. Chinese writings note that, given the importance of space systems for navigation, positioning, and timing, disruption of associated networks will result in the disruption of the OODA loop. Therefore, key point strikes in joint operations should seek to disrupt the enemy’s information collection and transmission nodes and command and control networks, through complementary hard and soft means. In the Chinese view, such attacks will cause the adversary’s integrated systems of systems to decohere.

The concept of “key point is space dominance” consequently emphasizes the importance of securing space dominance, through the comprehensive application of various types of tactics and forces, in a variety of ways, including interference, obstruction, disruption, and destruction of enemy space-related systems (including terrestrial facilities and data links). The objective is both to prevent the enemy from operating their space systems for as much of the course of the conflict as possible and also ensure that one’s own space systems can operate effectively. To this latter end, establishing space dominance also encompasses the exploitation of space, whether in the provision of

information support to terrestrial operations, undertaking space deterrence or engaging in operations against remaining enemy space assets (Jiang 2013, p. 44).

“Key point is space dominance” therefore has two meanings. On the one hand, it is reminding PLA officers and staff that an important priority must be securing space dominance over an opponent. Therefore, resources must be applied against an enemy’s space systems (terrestrial facilities, orbiting platforms, data links) to disrupt and deny an opponent the ability to exploit space. Moreover, these attacks must be sustained throughout the course of the conflict, but special attention should be paid to the first battle, where it is important to secure maximum effect as it is likely to influence the entire course of the conflict.

As important, one must also be prepared to defend one’s own space infrastructure, since the enemy is likely to be striving to secure space dominance as well. This will entail incorporating both hard and soft defenses, including deceptive measures and maintaining secrecy to mislead an opponent’s allocation of offensive measures, as well as hard defenses aimed at countering their attacks directly.

However, even with the full range of national space assets at one’s command, there remains only a limited resource base. Chinese analysts recognize that space systems are fragile; as important they are extremely expensive, so even wealthy nations are unlikely to have a substantial reserve of platforms. Nor do many nations have a multiple redundant terrestrial space launch and mission control network. (In this regard, it is worth noting that, with the inauguration of the Hainan Island spaceport, China will have four space launch facilities.) Therefore, the other aspect of “key point is space dominance” is that space operations need to be focused, with a specific focus, a key point, and not scattershot. Attacks against adversary space infrastructure need to be carefully coordinated and undertaken at essential moments in the overall campaign, to maximize effect.

---

## Space Dominance and Information Dominance

As information dominance has assumed a higher importance in Chinese thinking and as China has developed its own array of satellites, the relationship between establishing space dominance and information dominance has evolved. Chinese analysts have long recognized, since at least the first Gulf War 25 years ago, that space is a key means of providing information support to terrestrial forces. Consequently, the emphasis upon establishing space dominance, as part of the struggle for information dominance, has become more explicit.

Several PLA analyses, for example, have observed that space is the “strategic high ground (*zhanlue zhigao dian*; 战略制高点)” in informationized warfare. They conclude that the ability to dominate space will have greater impact on informationized warfare than any other domain, because it will provide:

- Real-time, global monitoring and early warning, such that no major military activity can occur without being spotted
- Secure, long-range, intercontinental communications

- Positional and navigational information that will support long-range, precision strike, including against targets that are over the horizon

All of these will occur without restriction from political borders, physical geography, or weather conditions and time of day (Ye 2007, p. 154; Chi and Xiao 2005, pp. 38–39).

Space dominance entails not only the ability to provide information support to the PLA but also to deny an adversary the ability to exploit space to gain information. The American reliance on space systems, in particular, has been remarked upon. One Chinese assessment notes high levels of American investment in military communications satellites, navigation satellite, reconnaissance and surveillance satellites, ballistic missile early warning satellites, and environment monitoring satellites (Xu 2013, p. 50). These satellite constellations, moreover, will be complemented by an array of terrestrial and aerial systems, to provide a complete, overlapping array of surveillance capabilities. The expectation is that the United States is preparing to disrupt, degrade, deny, and destroy adversary space systems in the effort to establish information dominance and conversely that the Americans are also preparing to face such attacks against their own systems.

Nor is American dependence upon space unique, in the Chinese view. PLA writings indicate that they are also closely observing other nations' space developments. Russian space developments in particular seem to garner heavy Chinese attention. The Chinese military textbook *Military Astronautics* discusses Russian as well as American aerospace forces (Chang 2005, pp. 219–220). The 2013 edition of *The Science of Military Strategy* observes that Russia has made space a major focus of its military refurbishment effort and that Moscow has increased its investments in the space sector as the Russian economy has improved (Academy of Military Science Military Strategy Research Office 2013, p. 180). In particular, Russian dependence on space systems has been noted. One Chinese volume related the Russian observation that “If Russia did not have an advantage in space, then it would not have reliable communications and reconnaissance, in which case, it would lack modernized information systems,” leaving Russia blind and deaf (Wu 2004, p. 102).

This will make the struggle for space dominance that much more pointed. Chinese authors believe that without space dominance, one cannot obtain information dominance and aerial dominance, and therefore one cannot achieve land or maritime dominance. Space will therefore inevitably be a battleground, if only in order to deny an adversary the ability to use it freely (Ye 2007, p. 154). Consequently, the space arena will be one of the very first scenes of conflict, as the two sides struggle for control of space. Neither side can afford to neglect this theater, as it will be a central determinant of who will secure information dominance (Chi and Xiao 2005, pp. 38, 39).

---

## Mission Areas Associated with Space Operations

PLA analysts believe that military space operations are likely to entail five broad “styles (*yangshi*; 样式)” or mission areas: space deterrence, space blockades, space strike operations, space defense operations, and provision of space information

support. (This section draws upon Jiang (2013, pp. 126–154).) It is important to recognize that such operations will most likely not be undertaken by themselves but in the context of a larger, joint campaign. Nonetheless, the purpose of all such operations is ultimately to affect information dominance by securing space dominance.

### **Space Deterrence (kongjian weishe; 空间威慑)**

Space deterrence is the use of space forces and capabilities to deter or coerce an opponent, preventing the outbreak of conflict or limiting its extent should conflict occur. Space deterrence is possible because of the growing importance of space-derived information in not only military but economic and social realms. By displaying one's own space capabilities and demonstrating determination and will, the PLA would hope to induce doubt and fear in an opponent over the prospect of loss of access to information gained from and through space and the resulting repercussions. This, in turn, would lead the adversary to either abandon their goals or else limit the scale, intensity, and types of operations (Zhou and Wen 2004; Academy of Military Science Military Strategy Research Office 2013, p. 181).

It is important to note here that the Chinese concept of space deterrence is not focused on deterring an adversary from conducting attacks against China's space infrastructure, per se. Instead, it is focused on employing space systems as a means of influencing the adversary's overall perceptions, in order to dissuade or compel them into acceding to Chinese goals. Thus, it is not so much deterrence *in* space, as deterrence *through space means*.

Space capabilities are seen as contributing to overall deterrent effects in a number of ways. One is by enhancing other forces' capabilities. Thus, conventional and nuclear forces are more effective when they are supported by information from space-based platforms, such as navigational, reconnaissance, and communications information. This makes nuclear and conventional deterrence more effective and therefore more credible.

In addition, though, space systems may coerce or dissuade an opponent on their own. Space systems are very expensive and hard to replace. By holding an opponent's space systems at risk, one essentially compels them to undertake a cost-benefit analysis. Is the focus of Chinese deterrence or coercive efforts worth the likely cost to an adversary of repairing or replacing a badly damaged or even destroyed space infrastructure? Moreover, because space systems affect not only military but economic, political, and diplomatic spheres, damage to space systems will have wide-ranging repercussions (Li and Dan 2002). Is the target of Chinese deterrent or coercive actions worth the impact of the loss of information from space-based systems on other military operations or on financial and other activities? The Chinese clearly hope that the adversary's calculations would conclude that it was better not to challenge Chinese aims. Even the threat of interference and disruption of space systems "will impose a certain level of psychological terror, and will generate an impact upon a nation's policy-makers and associated strategic

decision-making” (Academy of Military Science Military Strategy Research Office 2013, p. 181).

PLA teaching materials suggest that there is a perceived hierarchy of space deterrence actions, perhaps akin to an “escalation ladder” involving displays of space forces and weapons; military space exercises; deployment or augmentation of space forces; and employment of space weapons.

Displays of space forces and weapons (*kongjian liliang xianshi*; 空间力量显示) occur in peacetime or at the onset of a crisis. The goal is to warn an opponent, in the hopes of dissuading them from escalating a crisis or pursuing courses of action that will lead to conflict. Such displays involve the use of various forms of media to highlight one’s space forces and are ideally complemented by political and diplomatic gestures and actions, such as inviting foreign military attaches to attend weapon tests and demonstrations.

Military space exercises (*kongjian junshi yanxi*; 空间军事演习) are undertaken as a crisis escalates, if displays of space forces and weapons are insufficient to compel an opponent to alter course. They can involve actual forces or computer simulations and are intended to demonstrate one’s capabilities but also military preparations and readiness. At the same time, such exercises will also improve one’s military space force readiness. Examples include ballistic missile defense tests, anti-satellite unit tests, exercises demonstrating “space strike (*kongjian tuji*; 空间突击)” capabilities, and displays of real-time and near-real-time information support from space systems.

Space force deployments (*kongjian liliang bushu*; 空间力量部署) are seen as a significant escalation of space deterrent efforts. It occurs when one concludes that an opponent is engaged in preparations for war and involves the rapid adjustment of space force deployments. As with military space exercises, this measure is not only intended to deter an opponent but, should deterrence fail, is seen as improving one’s own preparations for combat. Such deployments, which may involve moving assets that are already in orbit and/or reinforcing current assets with additional platforms and systems, are intended to create local superiority of forces so that an opponent will clearly be in an inferior position. It may also involve the recall of certain space assets (e.g., space shuttles), either to preserve them from enemy action or to allow them to prepare for new missions. This may be akin to the evacuation of dependents from a region in crisis, as a signal of imminent conflict.

The Chinese term for the final step of space deterrence is “space shock and awe strikes (*kongjian zhenshe daji*; 空间震慑打击).” If the three previous, non-violent deterrent measures are insufficient, then the PLA suggests engaging in punitive strikes, so as to warn an opponent that one is prepared for full-blown, comprehensive conflict in defense of the nation. Such strikes are seen as “the highest, and final technique (*zuigao xingshi he zui hou shouduan*; 最高形式和最后手段)” in seeking to deter and dissuade an opponent. Employing hard-kill methods, soft-kill methods, or a combination, one would attack an opponent’s physical space infrastructure or data links, respectively. If this succeeds, opposing decision-makers will be psychologically shaken and cease their activities. If it fails, an opponent’s forces will nonetheless have suffered some damage and losses.



## **Space Blockade (kongjian fengsuo zuozhan; 空间封锁作战)**

Space blockades involve the use of space and terrestrial forces to prevent an opponent from entering space and from gathering or transmitting information through space. There are several different varieties of space blockade activities. One is to blockade terrestrial space facilities, including launch sites; tracking, telemetry, and control (TT&C) sites; and mission control centers. They can be disrupted through the use of kinetic means (e.g., special forces, missiles) or through computer and information network interference.

Another means is to obstruct orbits. This can include actually destroying satellites that are in orbit or else obstructing orbits, such as by creating clouds of space debris or deploying space mines. By threatening the destruction of adversary satellites (without necessarily doing so), one might limit the function of those satellites (e.g., by limiting their maneuvers). The risk, however, is that either such step might damage third-party space systems, which in turn could lead to strategic consequences. Therefore, this approach to imposing a space blockade imposes very high requirements for precise control, extremely detailed space situational awareness, and highly focused, limited deployment.

Another method is the obstruction of launch windows. If one can delay a launch, whether through interfering with its onboard systems or otherwise disrupting the schedule, then a satellite may not be able to reach its proper orbit. In the past, some American space launches have been delayed because fishing and pleasure boats were present down-range (Atlas 3 2000; Orwig 2014). This alternative also includes the possibility of a boost-phase intercept of a space launch vehicle.

Finally, one can impose an information blockade. By interfering with and disrupting an opponent's data links between terrestrial control stations and the satellite, one can effectively neutralize an orbiting satellite by hijacking the satellite's control systems or preventing ground control from issuing instructions. Alternatively, one can interfere with the data that the satellite is transmitting. That is, rather than tampering with the satellite's controls, one can contaminate or block the data that is passing through the satellite. A third form of information blockade involves "dazzling" a satellite, using low-powered directed energy weapons against sensors or other systems. In each case, the intent is to affect a "mission kill," whereby the satellite cannot perform its functions, but is not necessarily destroyed.

## **Space Strike Operations (kongjian tuji zuozhan; 空间突击作战)**

Essential to the credibility of space deterrence and the undertaking of space blockades is the ability to conduct space strike operations. Space strike operations involve space and other forces pursuing offensive operations against an enemy's space-related targets, whether in space, or on land, at sea, or in the air. They are therefore not strictly limited to attacks against the space infrastructure, and certainly not only against orbital platforms. In general, space strike operations are expected to be against vital strategic and operational space-related targets, i.e., "key points" (Jiang 2013, p. 137).

Space strike operations, in the Chinese view, are marked by “integrated operations; stealth and surprise; key point strikes; and rapid, decisive action.” Integrated operations reflect the need to coordinate space strike operations with land, sea, and air operations, to forge “integrated combat power (*zhengti weili*; 整体威力).” They should also be undertaken at key moments when the enemy least expects it, exploiting stealth. They should also incorporate unexpected methods and tactics, so as to not only maximize material damage but also to undermine the enemy’s morale. By employing a mixture of hard- and soft-kill methods, one can maximize stealth and generate additional surprise by confusing an opponent, making it harder to defend against.

Key point strikes are part of what might be the guiding thought for space operations in general. Here, the emphasis is on tightly focusing space operations and concentrating space forces along the main direction, at key times, against key targets in the enemy’s combat systems of systems. The goals should be to disrupt, attrit, and paralyze the enemy’s combat systems of systems, to prevent them from generating integrated capabilities (Jiang 2013, p. 142). This also requires carefully assessing an adversary’s space system and identifying those key systems and vulnerabilities, since neither side is likely to field large numbers of space systems.

Rapid, decisive action denotes the need to use space strikes to seize the overall initiative in a campaign. By overwhelming an opponent and then sustaining strikes afterward, one can not only retain the initiative but ideally achieve operational goals and conclude the conflict. At the same time, due to the limited numbers of space platforms and weapons likely to be available, their fragility, and their expense (which limits numbers acquired), space strike operations are likely to be of relatively limited duration.

In the Chinese conception, space strike operations involve attacks against the full range of enemy space-related systems. One central element is the enemy’s various satellite constellations. These can be targeted by a variety of hard-kill methods, such as directed energy weapons, kinetic kill vehicles (such as the one used in the 2007 anti-satellite test), and space mines and co-orbital anti-satellite systems (Chi and Xiao 2005, p. 39).

Equally important are such information warfare methods as “space electronic warfare and space network warfare (*taikong dianzi zhan he taikong wangluo zhan*; 太空电子战和太空网络战).” The application of integrated network electronic warfare (INEW) methods in space can interfere and disrupt the enemy spacecraft’s various systems, including its onboard computers and other electronic components. Such methods can achieve a “mission kill,” effectively neutralizing the platform, without generating the physical debris associated with collisions by kinetic kill vehicles and other physical attacks. Such soft-kill methods are seen as a vital means of conducting space information combat.

In addition, Chinese analyses suggest that striking at both space and terrestrial targets is necessary to establish local space superiority (Li et al. 2003). Such integrated attacks are comparable to traditional attacks against enemy command nodes or military bases (Hong and Liang 2002). Such attacks carry the additional advantage of retarding an opponent’s ability to reinforce or replace damaged or

destroyed orbiting systems. Therefore, Chinese analyses indicate that vital targets for securing space dominance include the ground components of the adversary's space systems, such as space launch vehicles and their launch sites and the attendant data and communications systems that link them together. Air, naval, ground, and special operations forces are therefore part of the arsenal of offensive space weapons, alongside ASATs and laser dazzling systems (Ma 2013, p. 220).

Chinese authors, however, also recognize that attacks against terrestrial targets, especially those based in the enemy's home territory, are likely to have significant strategic implications and potential repercussions. Therefore, attacks against strategic space targets require the direction of the highest-level political authorities.

Chinese analysts also believe that space strike operations will eventually include space-to-ground offensive operations, that is, the use of space-based weapons to bombard terrestrial targets. Some Chinese commentators, for example, have posited that the X-37B unmanned space vehicle might serve as a basis for a prompt global strike capability (Zhi and Li 2014). In this regard, they clearly see parallels between the development of space power and air power, i.e., the steady move from providing information support (aerial artillery observation, space-based reconnaissance and surveillance) to attacks against the adversary's information support systems, to the provision of fire support.

## **Defensive Space Operations (kongjian fangyu zuozhan; 空间防御作战)**

At the same time as conducting space information operations and space strike operations, the PLA also expects to undertake defensive space operations. These defend one's own space systems (including orbiting satellites, terrestrial facilities, and the associated datalinks) from attacks by enemy space or terrestrial weapons and also protect national strategic targets from attacks from space systems or ballistic missiles (Zhang and Li 2005).

Defensive space operations involve a combination of passive and active defensive measures. Passive measures involve making Chinese satellites harder to track or determine their function. Chinese writings suggest that space systems should, as much as possible, incorporate camouflage and stealthing measures, so as to hide the nature and functions of the spacecraft from opposing observation and probes (Chang 2005, p. 316). Other passive measures include deploying satellites into orbits designed to avoid enemy detection; employing political, diplomatic, and other channels to mislead opponents of real operational intentions or otherwise influence enemy decision-making; and deploying false targets and decoys, to overload opponents' tracking capacities.

Because it is difficult to hide objects in space for very long, the Chinese have also shown an interest in resilience, i.e., extending survivability of space systems even after they are discovered. Some Chinese writings have discussed the deployment of small- and microsatellites in networks and constellations, rather than single large systems. According to one Chinese analysis, employing larger numbers of much

smaller satellites may yield the same or greater capability than deploying a smaller number of larger, individually more capable systems, with less vulnerability (Bei et al. 2002). Larger satellites should be capable of functioning autonomously, so that even if their ground links are severed, they would nonetheless be able to continue operations (Chang 2005, p. 320). In addition, ground controllers should be prepared to move satellites, if there are indications that they might be attacked. Chinese planners may also be considering the incorporation of sufficient autonomy into satellites that they might be capable of altering their orbits on their own in order to evade perceived attacks.

Another set of survivability measures is the incorporation of hardening. This can only go so far, however, since spacecraft are very fragile. This is an inherent function of concentrating a number of sub-systems into a small volume and the extremely hostile environment of outer space, so that any damage to the spacecraft is likely to lead to substantial cascading effects (Xie and Zhao 2009). Similarly, while some ground facilities, including mission control facilities, might be physically hardened, the requirement for large antennae to handle telemetry imposes limits on how much physical hardening is possible.

In the Chinese view, defensive space operations cannot be solely reactive measures. As one PLA article notes, one can, and should, also employ offensive means and seek the initiative in the course of space defensive operations. More active defenses might include targeting enemy anti-satellite weapons, such as adversary co-orbital ASATs. Both offensive and defensive means, moreover, should be undertaken by not only space forces but also by land, sea, and air forces (Hong and Liang 2002). In the PLA's view, a combination of electronic and physical measures, including firepower strikes, may disrupt and suppress enemy space systems. By attacking terrestrial support components such as the TT&C facilities, the enemy's ability to conduct any kind of space operations, whether attacks against satellites or even provision of information support from space-based platforms, will be disrupted, thereby allowing one's own side to achieve space dominance.

It should be noted that the Chinese concept of "defensive space operations" does not necessarily parallel "defensive space control," as laid out in US Joint Publication 3-14 *Space Operations*. Indeed, some aspects would seem to overlap with that of "offensive space control" in the American sense (Joint Chiefs of Staff 2009, p. II-6).

### **Space Information Support Operations (kongjian xinxi zhiyuan zuozhan; 空间信息支援作战)**

In the 2005 edition of *Military Aerospace*, a PLA textbook on military space activities, provision of information support by space systems was listed as the second task, after space deterrence (Chang 2005, pp. 304–309). In PLA teaching materials published in 2013, provision of information support by space systems was now the fifth of five tasks. This would suggest that space information support operations, while still important, are being eclipsed by more active space offensive and defensive measures. Indeed, as one Chinese assessment observes, as space resources

become ever more important, and as military aerospace technology, especially those related to offensive space operations, steadily develops, space force development will shift from providing information support toward securing space dominance (Tan 2012, p. 170).

Nonetheless, in the context of informationized warfare, provision of space information support will be one of the greatest benefits of achieving space dominance. As the 2013 edition of *The Science of Military Strategy* notes, “space information support is now and for a long time into the future the main form (*zhuyao fangshi*; 主要方式) by which various nations apply space strength” (Academy of Military Science Military Strategy Research Office 2013, p. 181). As the PLA continues to emphasize joint operations, it will increasingly depend upon space-based systems to provide information support, especially as Chinese forces move farther and farther away from Chinese territory (and therefore, land-based information support infrastructure).

Key tasks within this mission area of “space information support (*kongjian xinxi zhiyuan*; 空间信息支援)” to the ground, air, and naval forces include:

- Space reconnaissance and surveillance
- Early warning of missile launches
- Communications and data relay
- Navigation and positioning
- Earth observation, including geodesy, hydrographics, and meteorology

While the priority accorded space information support may have fallen somewhat relative to other tasks such as space deterrence, providing this information to the other parts of the Chinese joint force remains essential. These capabilities are essential enablers for the PLA’s ability to coordinate forces, engage in precision strikes, and assess damage.

So long as the PLA’s main contingencies are on its immediate periphery (e.g., Taiwan, the Sino-Indian border), senior commanders will have a plethora of additional resources to gain information, ranging from unmanned aerial vehicles (UAVs), aircraft, and fishing boats to radio direction finding to terrestrial communications and sensor networks. But as the PLA’s activities extend farther from China’s shores (e.g., the Indian Ocean and Central Pacific), space will provide an increasing proportion of the information needed by Chinese military planners.

---

## Space and Information Dominance “Under the New Circumstances”

Chinese military analysts and planners have long emphasized “informationized conditions” will dominate future warfare, but even they did not foresee the extent to which information would evolve and permeate all aspects of conflict. The sustained growth in information and communications technology (ICT) has led to what is termed “the new circumstances (*xin xingshi*; 新形势).” These “new

circumstances” pose a range of challenges for defense planners, as weapons have become more precise, more intelligent, and more stealthy and are often autonomous. Moreover, the future battlefield will involve an ever-closer linkage between physical systems and electronic and virtual ones. “There will be basic changes in traditional concepts of time and space on the battlefield, as combat forms increasingly shift from mechanized towards informationized” (The Growing Importance 2016).

Especially important is the impact of these in ICT on the conduct of joint operations. The ability to establish dominance across the various domains, including land, sea, air, and the electromagnetic domain as well as outer space, will be much more difficult. Chinese writings have noted the importance of “multi-domain dominance” as part of the approach to future conflicts. But if commanders are able to achieve this, then their situational awareness will be far greater, given the various sensors and information systems at their disposal. At the same time, the ability to share information among the various participating forces, creating synergies among them, will make the side with multi-domain dominance virtually unassailable.

Consequently, the need to establish multi-domain dominance, centering around information dominance, is a central part of “the new circumstances.” Key ICT technologies, including artificial intelligence, big data, and cloud computing, are shaping these “new circumstances.” At the same time, however, space is a fundamental enabler of these ICT technologies, because of its central role in the acquisition and movement of information.

The development of massive constellations of Earth observation, communications, and data relay satellites, each with hundreds or even thousands of small-sats, will fundamentally alter the role of space in military operations. Such massive constellations may provide mobile access to broadband, allowing even more constant and rapid data flow. Proliferation of Earth observation satellites will make it much harder to conceal forces or hide development of new capabilities. These capabilities will further enhance terrestrial joint operations.

As important, denying space to an adversary will also be a growing priority, as it prevents an adversary from undertaking effective joint operations. Indeed, the growing significance apparently accorded space deterrence and space blockade, relative to space information support operations, in Chinese writings, suggests that PLA analysts consider space forces increasingly capable of exerting a *strategic* impact in their own right. In particular, the PLA appears to believe that by threatening adversary space capabilities, one can employ compellence strategies against those adversaries, in ways comparable to conventional and nuclear deterrence. This would appear to be yet another consequence of the “new circumstances.”

At the end of 2015, in order to address these “new circumstances,” the PLA undertook some of the most extensive and fundamental reorganizations since its founding in 1927. These embodied the ideas of “The Central Military Commission would manage the overall, the war zones would focus on warfighting, and the services would manage construction (*junwei guan zong, zhanqu zhuzhan, junzhong zhujian*; 军委管总, 战区主战, 军种主建)” (Xi Jinping 2015; Zhang 2016):

- The Central Military Commission, which manages the overall Chinese military, was reorganized from four General Departments to 15 departments, offices, and commissions. In the course of this reorganization, the General Staff Department has been renamed the Joint Staff Department, underscoring the heightened importance of joint operations for the PLA.
- The previous seven military regions (*junqu*; 军区) were consolidated into five theater commands or war zones (*zhanqu*; 战区). Where the previous military regions had been primarily peacetime entities with no wartime role, the new war zones are the operational-level command structures that are expected to undertake joint operations within their respective geographic areas of responsibility.
- The creation of three new services. The Second Artillery, previously a “super-branch,” was elevated to the level of a full-blown service. The ground forces, which had previously been the default, now became a separate service (the PLA ground forces or PLA Army), in a sense losing political clout as a result. And the PLA Strategic Support Force (PLASSF) was created.

The PLASSF, in particular, will affect how the PLA implements space operations.

### **Creation of the PLA Strategic Support Force (PLASSF)**

The PLASSF combined the PLA’s electronic warfare, network warfare, and space warfare capabilities. This included what had previously been specific departments under the General Staff Department (GSD), such as the GSD Third Department (responsible for signals intelligence) and the GSD Fourth Department (responsible for electronic intelligence and electronic warfare). It also involved the transfer of key space facilities that had been part of the General Armaments Department (GAD), including China’s launch sites; satellite control centers; tracking, telemetry, and control facilities; and China’s fleet of space surveillance ships. Because of the Chinese emphasis on influencing adversary commanders and staffs, some political warfare elements from the General Political Department have also been incorporated into the PLASSF.

One reason for the establishment of the PLASSF appears to be the shift from a task or mission-oriented approach to warfare (e.g., reconnaissance, strike) to one more focused on specific domains (Costello and McReynolds 2018, p. 12). The PLASSF, as a service, will be responsible for planning, force construction, and operations within the information domain, including space operations. While the GAD had space responsibilities, it was neither a military service nor a warfighting entity; the GAD’s main tasks were supporting military research and development, including new weapons, as well as managing China’s nuclear and space facilities. Creating the PLASSF effectively created a service that was more focused on space warfighting doctrine and forces, rather than space systems and capabilities.

Moreover, this new service is “intended to create synergies between disparate information warfare capabilities, in order to execute specific types of strategic missions” (Costello and McReynolds 2018, p. 5). By reorganizing the PLA’s basic

structures and combining various information-related departments, offices, and bureaus across the PLA, many of the organizational stovepipes that impeded programmatic and doctrinal coordination were effectively defanged. In the case of space operations, the PLASSF's Space Systems Department now oversees GAD space facilities but also units responsible for space-based C4ISR (such as space-based remote sensing) that had resided in the General Staff Department (Costello and McReynolds 2018, p. 20).

At the same time, by embedding the Space Systems Department alongside the Network Systems Department (the other main subordinate entity within the PLASSF), there is greater ability to integrate space operations with network warfare (including cyber warfare) and electronic warfare operations. Chinese writings emphasize the importance of electronic and network warfare as key means of establishing space dominance, as soft-kill (e.g., laser dazzlers, cyberattack methods against TT&C facilities and onboard systems) approaches are an essential complement to hard-kill (e.g., direct ascent anti-satellite missiles, co-orbital anti-satellite systems) ones. By placing all of these capabilities in the same service (albeit in separate subordinate departments), PLA space dominance efforts will benefit from enhanced coordination and integration.

## Civil-Military Integration of Space Industrial Capabilities

Another aspect of the “new circumstances” is the recognition that there must be greater civil-military integration, at not only the industrial level but also in terms of the broader organization of the nation's resources. This is reflected in the shift in Chinese terminology from “civil-military linkage” or “civil-military integration” (*junmin jiehe*; 军民结合) to “civil-military fusion” or “civil-military melding” (*junmin ronghe*; 军民融合). The idea of “fusion” or “melding” underscores the need to move beyond just linkages between the civilian and military sides. Instead, there must be a broader reorganization of the overall national economy and industry, so that the two sides are mutually served by a common economic base (Innovation Department 2019).

This has particularly significant importance in the space context, as the PRC has begun to support the development of additional commercial space capacity. Until recently, all Chinese aerospace industrial activity was undertaken by two state-owned enterprises: China Aerospace Science and Technology Corporation (CASC) and China Aerospace Science and Industry Corporation (CASIC). Beginning in 2015, however, the Chinese began to promote the development of non-state-owned space companies, with the promulgation of the “National Civilian-Use Space Basic Facilities Mid- and Long-Term Development Plan (2015–2025) (*guojia minyong kongjian jichu sheshi zhong chang qi fazhan guihua*; 国家民用空间基础设施中长期发展规划).” (It is important to note that “civilian use (*minyong*; 民用)” does not only mean **nonmilitary** use but can also mean **nongovernmental** use.)

This Plan was formulated by the National Development and Reform Commission, the Ministry of Finance, and the State Administration of Science, Technology,



and Industry for National Defense (SASTIND), the entity responsible for the military industrial complex (Xie et al. 2017).

The Plan laid out several specific goals for the coming decade:

- Supporting construction of civilian and commercially financed and supported satellite manufacturing and associated research and development programs.
- Linking the public interest and commercialization. Commercial ventures should rely on societal (i.e., nongovernmental) investment.
- Encouraging and supporting investment by wealthy enterprises in planned satellite systems (Mao 2017).

The Plan expects that the main areas of commercial development will be in satellite remote sensing, communications satellites, navigation satellites, and associated applications. Chinese writings suggest that they foresee especially robust growth in the communications satellite sector over the next 5–10 years (Guo 2017). These elements will be integrated into a unified set of space-ground networks that will support global provision of space-derived services and information.

Another area of interest will be commercial launch services. The development of the Kuaizhou solid rocket booster for launching small satellites is seen as facilitating a broader Chinese role in commercial space launch. The January 2017 Kuaizhou-1A launch of three satellites is described as the first time the Chinese have commercially launched more than one satellite at a time.

As important, some Chinese writers see a “Kuaizhou model” for promoting broader use of Chinese launch systems. The model emphasizes:

- Low cost.
- Customized or tailored launch services. Clients can either choose to purchase an entire rocket for themselves (the Kuaizhou-1) or be part of a group of launched satellites (the Kuaizhou-1A).
- Different commercial approaches. One can first sign a purchase order and then cooperate, or one can engage in cooperative development and then sign a purchase order (Rao 2017).

Some of these themes were further explored at a conference held on September 15, 2015. Described as China’s first conference on commercial space flight development, it reportedly brought together key departments and ministries, scientific research organizations, academics, as well as representatives from civilian and commercial enterprises. One of the conclusions from the conference was that commercial space travel and exploitation would be difficult, if not impossible, with current Chinese approaches to research and development (China Commercial 2015).

The PRC seems to be pursuing four broad paths for expanding its aerospace industrial capacity along increasingly commercialized lines: traditional state-owned enterprises (SOEs), traditional research and development facilities and institutions, private commercial enterprises, and Internet-associated enterprises. These efforts at developing an expanded commercial capacity will be overseen by the State

Administration for Science, Technology, and Industry for National Defense (SASTIND) Since SASTIND is the entity also responsible for overseeing the overall Chinese military industrial complex, it is likely to ensure that Chinese military requirements and capabilities are not slighted by any of these new commercial ventures.

For example, Chinese e-commerce giant Alibaba has begun to probe possible investments in space. In August 2015, Alibaba reportedly joined with NORINCO Corporation to establish a joint venture to explore possible linkages between the Internet and the Beidou position, navigation, and timing system (Feng 2015). Through cloud computing and advanced data management techniques, this would help improve Alibaba's services. NORINCO is known as China North Industries Group Corporation, Limited, and is also known as China Ordnance Industries Group Limited. It is a major manufacturer and exporter of military as well as civilian goods.

---

## Conclusions

For the PLA and Chinese security decision-makers, the Information Age and the Space Age are inextricably linked. Both have been heavily influenced by the growth in computing power and the role of telecommunications. This has gained impetus as ICT has a growing role in overall national power and especially military capability.

Chinese analyses of recent wars underscore the intimate relationship between these two realms when it comes to warfighting. Modern wars have demonstrated the close relationship between information and space, where space systems play a central role in the collection, transmission, and exploitation of information. Consequently, as one PLA analysis observes, "seizing the space information advantage as a high ground is the first decisive condition for seizing information dominance, space dominance, air dominance, naval dominance, land dominance, and therefore the initiative in wartime" (Lanzhou Military Region Headquarters 2003).

By dominating space, one gains an enormous advantage in terms of access to information and managing information flow. The side that dominates space thereby gains several key advantages.

- *The battlefield is much more transparent.* Combat forces can therefore be much more effective, since enemy and friendly dispositions will be known.
- *Command and control is much more precise and capable.* Because the battlefield is more transparent, commanders can respond in real-time or near-real time enemy actions, and widely separated units drawn from a variety of services can act in a highly integrated manner.
- *It makes noncontact, nonlinear warfare possible.* By dominating space, one has secured the most important portion of the battlefield that of information space. The more transparent battlefield, the facilitated command and control, enables long-range, precision strikes, against which the adversary is gravely disadvantaged in trying to counter. Friendly casualties are reduced, while one's actions are much more effective.

For Chinese military planners, these advantages are further enhanced by certain geographic and strategic realities. China, even now, is not oriented toward mounting extensive military operations far from its shores, but remains focused on such flash points as Taiwan, the Korean peninsula, the South China Sea, and the Sino-Indian border. For the PRC, the consistent concern since the 1980s has been on “local wars.” Such wars are not only limited in means but also are expected to occur mainly on China’s periphery.

Consequently, the PLA can bring to bear substantial resources, drawn from across the entire country if necessary, in order to establish information dominance. Mobilized civilian assets, ranging from fishing boats for maritime surveillance to the militia for camouflage and deception operations, can supplement regular PLA forces. Shorter-range assets from fast attack craft to older fighter aircraft can similarly be employed to deny and counter adversary forces, including information collection platforms. Communications can be sustained through fiber-optic cable (which is difficult to monitor), cell phones, line-of-sight radios, as well as satellite communications, enhancing communications security and providing redundancy. In many ways, China does not need space for the PLA to operate in accordance with its doctrine.

By contrast, the United States is an expeditionary military, operating far from American shores. In time of conflict, it is therefore much more reliant upon space-based systems even for operational communications, especially to coordinate disparate, separated forces, as well as for intelligence collection against targets typically halfway around the globe. As important, American military planners have chosen to rely on space-based assets for positioning, navigation, and timing, whether it is aircraft routing, shipborne navigation, or weapons guidance. The combination of geostrategic conditions and weapons acquisition policies makes American forces much more dependent upon space.

In short, in the struggle for information dominance, because of the asymmetric strategies and starting conditions, there is a resulting asymmetric dependence on space.

At the same time, it is important to recognize that the various space architectures are microcosms of the larger information battlefields. Space networks, encompassing the satellites, terrestrial support structures such as mission control, and the data links connecting them are themselves systems of systems bound together via information networks. Satellites require communications and data links, not only to carry information about various targets or to provide navigation and other updates but also to allow mission control to monitor the satellites’ status, adjust their orbits, update their software, and otherwise manage and control their operations. It is this tracking, telemetry, and control (TT&C) network, and the information flow over it governing the satellite constellations and linking them back to Earth, that allows space systems to operate. Damaging or affecting that flow can effectively neutralize the constellation or even allow an adversary to take control of one or more satellites. Its preservation is as important for securing information dominance as having the constellation provide information support to the various terrestrial struggles. The ability to deny the adversary not only information gathering and transmission but

satellite monitoring and control, that is, denying them information about oneself or information about their space assets, can be equally damaging to their larger ability to establish information dominance.

It is for this reason that the Chinese emphasize that space dominance entails not only targeting satellites but ground facilities such as mission control sites and the data links connecting them. The struggle for space dominance is, in fact, a part of the larger struggle for information dominance. It is the facet that occurs within the confines of the two sides' space architectures.

---

## References

- Academy of Military Science Military Strategy Research Office (2013) *The science of military strategy*. Military Science Publishing House, Beijing
- Atlas 3 Scrubbed to Tuesday. *Space Daily*, May 21, 2000. <http://www.spacedaily.com/news/eutelsat-00g.html>
- Bei C, Yang J, Zhang W (2002) Nanosatellite distributor design proposal. *Zhongguo Hangtian Bao*, August 23, 2002, p 4, in FBIS-CHI
- Chang X (2005) *Military astronautics*, 2nd edn. National Defense Industries Press, Beijing
- Chi Y, Xiao Y (2005) *Essentials of informationized warfare and information operations theory*. Military Science Publishing House, Beijing
- China Commercial Spaceflight Development Conference Opens in Beijing (2015). *Aerospace China*, no 10
- China: Missile Defense System Test Successful. *USA Today*, January 11, 2010. [http://www.usatoday.com/news/world/2010-01-11-china-missile-defense\\_N.htm](http://www.usatoday.com/news/world/2010-01-11-china-missile-defense_N.htm)
- Costello J, McReynolds J (2018) China's strategic support force: a force for a new era. INSS China strategic perspectives paper no 13. National Defense University, Washington, DC
- David L (2007) China's antisatellite test: worrisome debris cloud encircles earth. *Space.com*, February 2, 2007. <http://www.space.com/3415-china-anti-satellite-test-worrisome-debris-cloud-circles-earth.html>
- Feigenbaum E (2003) *China's techno-warriors*. Stanford University Press, Stanford
- Feng C (2015) China's Alibaba teams up with state-owned arms maker to develop positioning services as Beijing shuns GPS. *South China Morning Post*, August 19, 2015. <https://www.scmp.com/tech/science-research/article/1850807/online-shopping-king-alibaba-working-chinas-state-owned>
- Gao Y (chief editor) (2001) *Joint campaign course materials*. Academy of Military Science Publishing House, Beijing
- Gao Q (2005) Aerospace reconnaissance characteristics and limits in high-tech local wars. *J Acad Command Equip Technol XVI*(1)
- Gruss M (2015) Space surveillance satellites pressed into early service. *Space News*, September 18, 2015. <http://spacenews.com/space-surveillance-sats-pressed-into-early-service/>
- Guo J (2017) Our nation's commercial aerospace shifts towards industrialization. *Economics Daily*, September 5, 2017. [http://www.gov.cn/xinwen/2017-09/05/content\\_5222713.htm](http://www.gov.cn/xinwen/2017-09/05/content_5222713.htm)
- Guojia Gao Jishu Yanjiu Fazhan Jihua 863. FBIS-CHI, July 21, 2000
- Hartnett D (2008) *Towards a globally focused Chinese military: the historic missions of the Chinese armed forces*. CNA Corporation, Alexandria
- Hong B, Liang X (2002) The basics of space strategic theory. *China Military Science*, no 1
- Hu J (2004) See clearly our military's historic missions in the new period of the new century, December 24, 2004. <http://gfjy.jxnews.com.cn/system/2010/04/16/011353408.shtml>
- Innovation Department, Beijing University Science and Technology Park (2019) *An outline of the development of our nation's civil-military fused enterprises*. China New High-Technology

- Enterprise Guiding Paper, April 15, 2019. <http://www.chinahightech.com/html/paper/2019/0415/521151.html>
- Jiang L (2013) Space operations teaching materials. Military Science Publishing House, Beijing
- Joint Chiefs of Staff (2009) Space operations, JP 3-14. Department of Defense, Washington, DC
- Lanzhou Military Region Headquarters Communications Department (2003) Space information support and its influence on future terrestrial operations. Military Art, no 10
- Li D (1999) A survey of the development of space technology in China. China Aerospace, June 1999, pp 16–19, in FBIS-CHI, September 21, 1999
- Li Y (2012) Joint campaign teaching materials. Military Science Publishing House, Beijing
- Li J, Dan Y (2002) The strategy of space deterrence. China Military Science, no 1
- Li D, Zhao X, Huang C (2003) Research on concepts of space operations and its command. J Acad Equip Command Technol XIV(5)
- Liu K, Wang X (2008) The first conflict won through airpower: the Kosovo war. Academy of Military Science Publishing House, Beijing
- Lu J (2008) Lu Jin: satellite communications – the information bridge during earthquake relief operations. Speech before the Chinese Communications Studies Association, September 26, 2008. <http://www.ezcom.cn/Article/8591>
- Ma P (2013) Joint operations research. National Defense University Publishing House, Beijing
- Mao L (2017) Development state of the main domestic commercial aerospace enterprises. Satellite Applications, no 10
- Matthews W (2010) Chinese puzzle. Defense News, September 6, 2010. <http://www.defensenews.com/story.php?i=4767907>
- Orwig J (2014) A rocket launch Monday was delayed because of a boat. Business Insider, October 28, 2014. <http://www.businessinsider.com/why-rocket-launch-delayed-by-a-boat-2014-10>
- PLA Encyclopedia Committee (1997) Chinese military encyclopedia. Military art, vol III. Academy of Military Science Publishing House, Beijing
- PLA Encyclopedia Committee (2002) Chinese military encyclopedia, supplemental volume. Military Science Publishing House, Beijing
- Rao H (2017) Commercial space: a necessary choice for major aerospace nations. National Financial Report, no 12
- Tan R (2012) Operational strength construction teaching materials. Military Science Publishing House, Beijing
- The Growing Importance of the Basic Factors in Strengthening National Defense and Army Building Under the New Circumstances. PLA Daily, August 2, 2016. [http://www.xinhuanet.com/politics/2016-08/02/c\\_129198048.htm](http://www.xinhuanet.com/politics/2016-08/02/c_129198048.htm)
- Wang H, Zhang X (chief editors) (2000) The science of campaigns. National Defense University Publishing House, Beijing
- Wang W, Zhang Q (2009) Discussing military theory innovation with Chinese characteristics. National Defense University Publishing House, Beijing
- Weeden B (2014) Through a glass darkly: Chinese, Russian, and American anti-satellite testing in space. Secure World Foundation, Washington, DC
- Wu R (2004) Theory of Informationized conflict. Military Science Publishing House, Beijing
- Xi Jinping (2015) Xi Jinping: form a structure where the central military commission manages the overall, the war zones focus on warfighting, the services manage construction. PLA Daily, November 26, 2015. <http://news.sohu.com/20151126/n428330471.shtml>
- Xi Jinping Repeatedly Supports Building a Major Aerospace Power. Xinhuanet, April 12, 2019. [http://www.xinhuanet.com/politics/xxjxs/2019-04/12/c\\_1124357478.htm](http://www.xinhuanet.com/politics/xxjxs/2019-04/12/c_1124357478.htm)
- Xie Z, Zhao D (2009) On the fundamental features of the military space force. China Military Science, no 1
- Xie P, Zhou X, Wang Y, et al (2017) A review of aerospace enterprise development during the ‘12th Five Year Plan’. National Development and Reform Commission, Department of High Technology Industry. [http://gjss.ndrc.gov.cn/ztp/xyqzlxhg/201708/t20170802\\_856978.html](http://gjss.ndrc.gov.cn/ztp/xyqzlxhg/201708/t20170802_856978.html)

- Xu G (2013) Research on our military's information operations strength construction. Military Science Publishing House, Beijing
- Ye Z (2007) Concepts of informationized operations. Military Science Publishing House, Beijing
- Yuan W (2008) Science of military information. National Defense University Publishing House, Beijing
- Zhang Y (chief editor) (2006) The science of campaigns. National Defense University Publishing House, Beijing
- Zhang X (2016) There is no natural boundary between war zones focus on warfighting, services manage construction. PLA Daily, March 21, 2016. [http://www.xinhuanet.com/mil/2016-03/21/c\\_128816639.htm](http://www.xinhuanet.com/mil/2016-03/21/c_128816639.htm)
- Zhang Q, Li X (2005) Space warfare: from vision to reality. China Military Science, no 1
- Zhang Y, Dong Z, et al (2005) Informationalized warfare will make seizing the aerospace technology 'high ground' a vital factor. People's Liberation Army Daily, March 30, 2005
- Zhi T, Li W (2014) X-37B, the mysterious space fighter. China Youth Daily, November 3, 2014. [http://jz.chinamil.com.cn/n2014/tp/content\\_6209028.htm](http://jz.chinamil.com.cn/n2014/tp/content_6209028.htm)
- Zhou P, Wen E (2004) Developing the theory of strategic deterrence with Chinese characteristics. China Military Science, no 3



# Historical Evolution of Japanese Space Security Policy

# 30

Kazuto Suzuki

## Contents

Introduction .....	556
The Diet's 1969 Resolution on "Exclusively Peaceful Purposes" .....	556
The End of the Cold War Paradigm .....	557
The Information-Gathering Satellite Program: Treading a Narrow Path Through a Legal Jungle .....	558
Kawamura's Initiative to Modify the 1969 Resolution .....	559
Legalizing the Strategic Objectives of Space Policy .....	560
Regional and Global Security .....	562
Changes of the Role of the Ministry of Defense .....	563
JAXA's View on Space Security .....	565
Japanese Reaction to the Code of Conduct .....	566
Conclusion .....	568
References .....	569

## Abstract

Japanese perspective on space security has begun with a very unique setting. The 1969 Diet Resolution has put heavy constraints on its space activities, and interpretation of "non-military" approach has refrained Japan from anything related to security. However, the 1998 Taepodong launch and subsequent reform of space policy eventually created Basic Space Law in 2008. Although the organizational culture and history still influence on the decision-making process, changing security environment and the role of Japan in the Asia-Pacific region made Japan to be more active and committed to both security by and of space.

---

K. Suzuki (✉)  
Hokkaido University, Hokkaido, Japan  
e-mail: [kazutos@juris.hokudai.ac.jp](mailto:kazutos@juris.hokudai.ac.jp)

## Introduction

The concept of space and security has been inconsistent for a long time in the history of Japan. Any space activities should be considered as peaceful one, which meant to be a place where military shall not play any part of it. This extreme interpretation of “exclusively peaceful purpose” has been challenged by many incidents concerning the security environment around Japan, and eventually reinterpreted through the discussion on the Basic Space Law in 2008. However, the older interpretation of “non-military use of space” is still persistent in Japan (Aoki 2008).

This chapter discusses the reasons why space and security were not compatible in Japan and analyzes the recent developments on the issues of space security. This chapter defines that the concept of “space security” does not limit to the issue of “security of space environment” but also includes “security on the earth through space systems.”

---

## The Diet’s 1969 Resolution on “Exclusively Peaceful Purposes”

Japan has restricted itself from using space for its security needs. As one of the most advanced industrialized country, Japan possesses technological and industrial capability to use space for its national security. Many non-Japanese space experts may wonder why it has not done so, if only for non-aggressive purposes.

The main reason for Japan’s reticence is its pacifist constitution, which is interpreted to prohibit using space for security purposes. In 1969, the Japanese parliament, the Diet, passed a resolution “Concerning the Principle of the Development and Utilization of Space,” popularly known as “the exclusively peaceful purposes resolution.” It stipulates that Japan’s space programs may be conducted by the civilian sector, not the defense sector, and only for the research and development of new technology for exclusively peaceful purposes (Suzuki 2005).

The principle of “exclusively peaceful purposes” is not new, as it appears in the Outer Space Treaty and the ESA Convention. The Japanese application of this principle, however, was unique. While debating the resolution in the Diet in 1969, the Diet members argued that it should be applied to the development and use of space in the same way that nuclear technology had been. As dual-use technology, they can be developed simultaneously for both civilian and military purposes. In addition, because Japan’s Science and Technology Agency (STA, currently MEXT) was in charge of both nuclear and space technology, the Diet felt that the development of space should be restricted as tightly as that of nuclear technology was. Ever since the horror of the nuclear holocausts in Hiroshima and Nagasaki, the Japanese people have been skeptical of using nuclear technology even for peaceful purposes, and therefore the Diet stipulated that it be used only for civilian purposes and that the military not be involved administratively, financially, and politically in its development and operation. (Response by Masao Yamagata, member of the Space Activities Committee, in the Special Committee of the Promotion of Science and Technology,



Lower House, minutes, April 16, 1969.) Accordingly, this notion of “exclusively peaceful purposes” was applied to space as well.

Based on the interpretation of the Diet resolution, all of Japan’s operations in space have been conducted for scientific and technological purposes. The strategic goal of Japan’s space policy thus has been to “catch up” with the technology of other advanced countries such as the United States and European nations. Thus, the goal of most of Japan’s space programs, even that of those for communication, broadcasting, and meteorology, has been technological excellence. For many politicians, space was the “necktie of advanced countries” (Matsuura 2004), suggesting that Japanese space policy should aim at gaining national prestige.

The principle of “non-military” use of space has changed, however, in accordance with the Basic Space Law which passed the Diet in June 2008. The aim of the law is to redefine the purpose and rationale for Japan to invest in space, and for the first time, the term *security* appears in an official document pertaining to space. Why has the notion of security suddenly appeared in the draft law, and how is it likely to change Japan’s space policy?

---

## The End of the Cold War Paradigm

For many years, particularly during the Cold War, Japan’s strictly “non-military” use of space was not challenged. The reason was that the alliance between Japan and the United States already provided the necessary infrastructure for telecommunication and intelligence gathering from space. In addition, Japan’s pacifist Constitution was interpreted as prohibiting its Self-Defense Forces (SDF) from being deployed beyond its national border. When the Cold War ended, however, Japan was forced to begin thinking about changing its space strategy (Suzuki 2007a).

With the end of the Cold War, the threat of Communism had waned, and so the reason for stationing US troops in Japan also had become less compelling as well. Although the United States still maintains a need for forward deployment bases in Japan, it is no longer a condition of the alliance. The unilateral collective defense – according to which the United States is obliged to defend Japanese territory but Japanese forces are not obliged to protect American territory or even US Forces – has now become too great a burden, so the US government wants the Japanese government to share more of responsibility for global security. Accordingly, Japan has enlarged its participation in the UN peacekeeping operations and the war on terror, particularly by deploying naval forces to support the multinational anti-terrorist operations in Afghanistan and its own ground troops in Iraq.

It is through these operations that the Self-Defense Forces have come to realize their technological shortcomings. Because the SDF are restricted from developing and operating their own space capabilities, they have had to rely on commercial satellite communication and commercial imagery services. But until now, because the SDF have not been permitted to be deployed outside Japan’s borders, they have not needed long distance communication or imagery of foreign countries other than its neighbors. However, the SDF have recognized the gap in Japan’s military

technology, particularly in regard to the United States' military transformation in recent years. Given the increasing possibility of Japan's sharing its security burden and joint operations with US forces, the SDF and the Japan Defense Agency (JDA, now the Ministry of Defense) now acknowledge the importance of developing their own space capability.

In addition, the Japanese people's perception of their security has been dramatically changed by North Korea's launch of a Taepodong missile over Japanese territory in 1998. The alarmed Japanese public thereupon demanded that the government take measures to protect them, and the government immediately decided to launch what is known as the Information-Gathering Satellite (IGS) program.

---

### **The Information-Gathering Satellite Program: Treading a Narrow Path Through a Legal Jungle**

At the start, the IGS program faced the serious legal constraints of Japan's space policy. Although it was clear that the purpose of the IGS program was to monitor the military activities of its neighbors, including North Korea, this was concealed under the guise of a "multipurpose" satellite program. This way the civilian nature of the program was implied in order to comply with the 1969 Diet resolution.

But this arrangement ran into problems. In the 1980s when Japan and the United States were sparring over trade, the US government pressured Japan to open its public procurement market in order to reduce the US trade deficit. The industry targeted was the space satellite industry, in which Japanese companies enjoyed exclusive contracts with the National Space Development Agency (NASDA, now the Japan Aerospace Exploration Agency, or JAXA). The US government maintained that it was unfair to exclude its satellite industry from competitive bidding and if Japan does not open up satellite procurement process to international bidders, the US government threatened to use its "Super 301" measure (imposing retaliatory tariff on Japanese products according to the Omnibus Foreign Trade and Competitiveness Act of 1988), according to which the US government could impose punitive tariffs on Japanese imports. In response, the Japanese government enacted the 1990 Accord on Non-R&D Satellite Procurement. The accord obliged the Japanese government to open the procurement market for civilian satellites to international competitive bidding, and as a result, 18 of a total 19 civilian non-R&D satellites in orbit were contracted to American companies, and only 4, the MTSAT-2 (meteorological and navigation satellite), Himawari 8 and 9 (Meteorological satellites) and Superbird-7 (commercial communication satellite), was contracted to a Japanese company. However, the launch of Quasi-Zenith Satellite System (QZSS) of which the first satellite was launched in 2009 has changed the dynamics. They are non-R&D satellites but procured by the government. The US government encouraged Japanese government to develop QZSS as supplementary system for its GPS.

As a result of the 1990 accord, the civilian multipurpose non-R&D satellites under the IGS program were part of the open procurement procedure as well, which

put the Japanese government in a difficult position. If it wanted to avoid applying the 1990 accord, it would have to admit that the “multipurpose” satellites under the IGS program actually had a military mission, a position that would violate the 1969 Diet resolution.

This problem was resolved by careful legal interpretation. The government placed control of the satellites not under the Japan Defense Agency (JDA) but under the Cabinet Secretariat, a small office with a national intelligence-gathering mission and crisis management functions. The IGSs then were formally designated as “crisis management satellites” with both civilian and military purposes (Sunohara 2005).

This incident made politicians realize that the legal constraints of the “exclusively peaceful purposes” resolution allowed no room for maneuver and that in the changing security environment of the post-Cold War period it seemed counterproductive to maintain such a rigid pacifist position.

The Koizumi government’s decision in 2003 to participate in the missile defense program raised another problem for Japanese space and security community. If JDA depended completely on US intelligence for initiating the deployment of counterattack missiles, it might mistakenly shoot down hostile missiles flying toward US territory. And because shooting down hostile missiles aimed at US territory would be an exercise of the right of collective self-defense by Japan, which is considered unconstitutional, it needed to have its own early warning satellite to verify the US satellite intelligence. Thus, many people in the Liberal Democratic Party (LDP), particularly those interested in defense issues, demanded a reconsideration of the “exclusively peaceful purposes” clause of the 1969 Diet resolution.

---

### **Kawamura’s Initiative to Modify the 1969 Resolution**

Despite the increasing demand to modify the resolution and the mounting pressure to reduce the space budget, neither the government nor the politicians took any action until the end of 2004. In early 2005, Takeo Kawamura, LDP politician and a former Minister for Education, Culture, Sports, Science, and Technology (MEXT), took the initiative for change. While he was Minister, Kawamura witnessed the failure of the H-IIA no. 6 launch carrying two IGSs. Although he was responsible for the actual launch on the H-IIA and not the IGS program, both the public and the government accused him for not properly supervising a strategically important satellite project like the IGS. From Kawamura’s standpoint, JAXA was responsible only for research and development, and it is acceptable, for R&D agency, to fail launch attempts because it is R&D rather than operational program. However, the Cabinet Secretariat, the operator of the IGS, was extremely furious about the failure of launching two IGSs which are vitally important for the national security. Yasuo Fukuda, Chief Cabinet Secretariat and No. 2 in the government, blamed Kawamura and JAXA for being irresponsible, and he claimed that it is not acceptable for JAXA to have excuse that launcher was only for R&D purposes. To Kawamura, this was a critical failure of Japan’s national strategy, and he was convinced that something had to be done (Suzuki 2007b).

As soon as Kawamura left his post as Minister of MEXT in September 2004, he convened an informal study group, the Consultation Group for National Strategy for Space, popularly known as the Kawamura Consultation Group. It was made up of members of LDP, including vice ministers in MEXT, the Ministry of Economy, Trade and Industry (METI), the JDA, and the Ministry of Foreign Affairs (MoFA). The Kawamura Consultation Group considered the problems of Japanese space policy, including the modification of the 1969 resolution and several public-private partnership programs such as the Quasi-Zenith Satellite System (QZSS), as well as the privatization of H-IIA (Suzuki 2006).

After ten meetings, the Kawamura Consultation Group issued an over 100-page report in October 2005, which argued that Japan's space policy lacked a coherent strategy and a clear institutional arrangement (Consultation Group for National Strategy for Space 2005). That is, because Japan's space policy was dominated by the Science and Technology Agency and MEXT, it did not have a plan for using space to pursue its national strategic objectives. The result was a lack of competitiveness in the Japanese space industry and the difficulty which Japan was facing in assuming a larger role on the international stage.

The report therefore suggested drafting a new space policy and an institutional framework within which a more coherent space policy could be formulated. First, it proposed that the government create a new minister for space in the office of the Cabinet, who would serve as the center for Japanese space strategy. Furthermore, the report pointed out that Japanese space policy had been to develop new technology but that along the way it had neglected the users' needs and demands. The report thus recommended that the new minister for space should bring relevant ministries into the policy-making process and refer their needs to the R&D program. The minister of space also should be authorized, the report continued, to use Japanese space assets to advance foreign and security policy purposes under the current constitutional framework.

The Kawamura Consultation Group's report also proposed the modification of the 1969 resolution. It suggested that any modification of the resolution would have to come from the Diet because the resolution was unanimously taken by the Diet, and the only way to legitimize the modification should be done through new resolution or legislation. Consequently, members of the LDP and the government were pleased with the report, as it paved the way for Japan to change its space policy.

---

## **Legalizing the Strategic Objectives of Space Policy**

Kawamura also submitted this report to the LDP's Policy Research Council. With support from Hidenao Nakagawa, then the Chairman of the Policy Research Council and the third-ranking member of the LDP, Kawamura established the Special Committee on Space Development (SCSD) with himself as its leader. In July 2006, when North Korea conducted a second missile test, the SCSD got another boost of support as public opinion quickly shifted from guarding its pacifist principles to demanding a more flexible interpretation of the 1969 resolution. In this

atmosphere, the SCSD decided to submit to the Diet its draft Basic Space Law in June 2007. The bill was sponsored not only by the LDP but also Komeito, its coalition partner, and Democratic Party of Japan (DPJ), the largest opposition. The reasons of DPJ sponsoring the bill was largely due to the belief of Kawamura that space is a national strategic issue and should not become a subject of partisan politics. He took initiative to invite Yoshihiko Noda, then the leader of Science and Technology policy group of DPJ and later became Prime Minister, to join the LDP sponsorship and Noda agreed. The participation of DPJ, largely composed by liberal and pacifist politicians, was important because it would guarantee that this bill will remain the pacifist nature of the space policy. Also, bipartisanship gave stability and continuity of space policy after the change of government in 2009. The bill passed the Diet in June 2008.

The first and the most important feature of the Basic Space Law is its institutional renovation, in accordance with the Kawamura Consultation Group's report. It proposes establishing a new Minister for Space and a Strategic Headquarters of Space Policy (SHSP), which will serve as Cabinet-level inter-ministerial coordination and decision-making body. The idea of establishing high-level political body is to make sure that the R&D activities and utilization of space systems will be seamlessly coordinated. For many years, Japanese space programs were decided based on the technological interests and "catch-up" to other space-faring nations. However, under the heavy budgetary constraints, the government could not afford to spend large sum of money only for the sake of technological development. In order to secure and sustain space budget, the government has to prove that the investment in space is effectively contributing to the policies and services to the people. The Minister for Space will be coordinating space-related policies of various ministries. One such ministry is the Ministry of Foreign Affairs (MoFA), which formulates policies to make Japan as leading state for setting new international rules by taking advantages of Japan's space technology as part of its foreign policy.

The second feature of the Law pertains to security. Article 2 of the Law states that "Our space development shall observe the Outer Space Treaty and other international agreements and shall be conducted in accordance with the principle of pacifism upheld in the Constitution." In other words, the traditional interpretation of "exclusively peaceful purposes" as "non-military" should no longer apply. Instead, the policy should be to adopt the international standard interpretation of the "peaceful use" of space as the "non-aggressive" or "non-offensive" use of space. The new Law would accordingly enable the Japanese defense authority to become involved in the development, procurement, and operation of space systems.

In addition, Article 3 states that "the government shall take necessary measures to promote space development that will contribute to international peace and security and also to our nation's security." Because this statement is so general, Article 3 could be interpreted as allowing the government to use space systems for aggressive purposes. But because Article 2 stipulates that the use of space systems for national and international security comply with both the framework of international agreements and Japan's constitution, it implies that Japan may use its space assets for crisis management and disaster monitoring in Asia and for peacekeeping missions

outside its territory. Article 2 also suggests that Japan can use early warning satellites for its missile defense, as this falls into the category of self-defense (Aoki 2009).

The Law therefore is designed to strengthen Japan's capability in settling disputes and managing crises by peaceful means and is intended to change only the interpretation of the Diet resolution, preventing any use of space by Japan's military authority.

---

## Regional and Global Security

With the Basic Space Law, the government will at last have a legal base for using space to strengthen its national security and expand diplomatic activities. This combination of security and diplomacy is important for two reasons. First, one of Japan's primary objectives of using space for security is to acquire the capability to defend its own country, particularly by means of a missile defense system. Given the small size of Japan's territory, space is not a very useful tool. It may not require a constant surveillance and communication capability. However, in the context of Japan's expanding role in international security and the Japan-US alliance, the SDF operations far from home would require long distance telecommunications and satellite intelligence. Such needs were confirmed by the Maritime SDF ships sent to the Indian Ocean to support the United States or to protect commercial vessels from piracy in the Gulf of Aden, and allied operations in Afghanistan as well as the Ground and Air SDF troops sent to Iraq.

The first SDF forces deployed outside Japan were sent to Cambodia in 1992 for UN peacekeeping missions. Since then, Japanese troops have been sent to places such as the Golan Heights, Mozambique, Zaire, East Timor, and South Sudan. Now the majority of Japanese no longer doubt their country's intention to contribute to international security and peace through UN operations, and consequently, the 1969 resolution has become both awkward and irrelevant. Although it states that space should be used for "exclusively peaceful purposes," during their UN operations, the SDF have not been allowed to use Japan's space assets to maintain "peace." The new law would not only enhance the scope of operation and capability of Japanese contribution to global security but it would also increase the efficiency and effectiveness of its participation in multinational operations.

Second, the combination of security and diplomacy in the new Law is important because Japan would be able to change Asia's security environment in Asia. A number of issues are causing instability and threatening the security of the region, particularly North Korea's nuclear and missile tests, tensions between Taiwan and China, China's opaque security strategy and defense budget, China's ASAT test in January 2007 (Hagt 2007), and various territorial and resource disputes. Although these conflicts have been contained by larger international organizations like the Association of Southeast Asian Nations (ASEAN) or ASEAN Regional Forum (ARF), they still need to be closely monitored to develop confidence building measures to ensure stability in the region and to seek peaceful solutions. Japan is, of course, the concerned party in some of these conflicts and needs to participate in such regional forums as ARF, the Asia-Pacific Economic Cooperation (APEC), and

the East Asian Summit. Although it is committed to providing ideas and resources for their development, Japan needs first to prioritize the promotion of regional interests as well as its own domestic interests. Japan also uses its technological advantages to assume a leadership role in the region. To date, it has been providing its technological expertise through the Asia-Pacific Regional Space Agency Forum (APRSAF). Japan has been playing a central role in APRSAF, but this was mostly done by the MEXT and JAXA without coordinating with the Ministry of Foreign Affairs. Thus, Japanese initiative focused purely on technical cooperation and has not fully incorporated with Japanese diplomatic strategy (Suzuki 2012a). However, the establishment of the Basic Space Law changed this lack of coordination. The Ministry of Foreign Affairs has created the “Office of Space” under the Foreign Policy Bureau and assigned several diplomats to dedicate their efforts to utilize space systems and activities for the diplomatic affairs.

---

## Changes of the Role of the Ministry of Defense

Due to the establishment of the Basic Space Law, the role of the Ministry of Defense (MoD) has changed dramatically. It has been excluded any space activities until 2008, except the use of satellite communications, broadcasting, and weather imageries. Although the 1969 Resolution has prohibited the JDA and later MoD to develop, own, operate, and use space systems, the government expressed its interpretation of the resolution in 1985 as follows:

The clause “exclusively peaceful purpose” in the Diet resolution means, of course, the SDF would not use satellites as lethal or distractive means, but also the use of satellite which is not generally available. In this context, the use of satellite, which is generally available and utilized, or possessing equivalent function to commercially available satellites, can be used by the Self-Defense Force. (Kato 1985)

Under this interpretation, the SDF was able to “use” satellite systems but still not allowed to “develop, own, and operate” them. However, the Basic Space Law urges that the government shall use space system “to ensure international peace and security and also to contribute to our nation’s security” (Article 3). This suggests that the MoD may develop, own, operate, and use space system for the purpose of international peace and security such as UN peacekeeping operations or national security. Nevertheless, the MoD was not given full-fledged space capability. The Article 2 defines that “Our space development shall observe the Outer Space Treaty and other international agreements and shall be conducted in accordance with the principle of pacifism upheld in the Constitution.” In other words, space activities of MoD shall remain within the framework of Japanese Constitutional constraints, which limits its military capability solely for self-defense. It means that the new interpretation of the use of space system for security purpose remains for passive use of space such as telecommunications, surveillance, and navigation, and even the case

of surveillance and reconnaissance, it would not be acceptable to use satellite intelligence for aggressive purposes.

The executives of the MoD were not very enthusiastic to invest in space for several reasons. First, under heavy budgetary constraints, MoD had to invest in a lot of new defense equipment to counter the modernized and upgraded Chinese forces. Also, the missile defense programs needed to be upgraded for the increasing threats from North Korea. In order to meet these challenges, there was no luxury to increase spending for unfamiliar domain of space. Second, due to the long period of refraining from the investment in space, MoD has almost no staff or technical expertise in space technology that eventually make MoD to depend on JAXA. Given the secretive nature of MoD, it would be difficult to depend on civilian agency to develop military sensitive technology. Although there is gradual rapprochement between MoD and JAXA, the level of cooperation is not satisfactory. For these reasons, the role of MoD was limited even after the establishment of the Basic Space Law.

Nevertheless, there were some pressing needs for MoD to take action in space domain. The first priority was to develop telecommunication satellites. Since 1985 government decision to allow SDF to use generally available satellite services, MoD has been using commercial satellite telecom services. The Sky Perfect JSAT, commercial operator, had satellite with X-band transponder dedicated to the use of SDF, but this satellite will reach the end of life by 2015. Thus, MoD needed to replace this satellite capacity with some other new services. Given the budgetary constraints and the lack of expertise, MoD decided to follow the British Skynet military communication satellite procurement model. The Skynet system was procured by British MoD as Private Finance Initiative (PFI) that means the commercial operator develop, manufacture, launch, and operate the satellite system and the MoD spend money only on services (Suzuki 2006). In this way, the MoD does not have to invest in developing human resources and technical expertise for building and operating satellites. The contract was awarded to the consortium led by Sky Perfect JSAT in 2012 and the satellite was launched in 2017 (now called “Kirameki”).

The second priority is the Space Situational Awareness (SSA). It seems strange for MoD to pay attention of SSA because it does not own or operate space assets. Even for civilian programs, most of JAXA's assets are developed as R&D satellites, so that they are not operational satellites (even the satellites such as ALOS series are classified as technology developing satellites). There are commercial and operational satellites for telecommunications, broadcasting, and meteorology, but these are located at Geostationary Orbit and the MoD does not take them as the assets to be protected. However, in the context of US-Japan alliance, SSA became important issue for MoD to deal with. Since the Basic Space Law passed the Diet in 2008 – 1 year after the Chinese ASAT test – the US government welcomed the new approach that Japan would invest in security-related programs in space and asked to participate in the construction of international network of SSA. Japan is strategically located to monitor airspace of West Pacific/East Asia, and the SSA data from Japan would complement the US's own SSA stations (Suzuki 2012b).



In this circumstance, MoD approached the SSA issue reluctantly. On the one hand, it recognizes that the SSA capability is important for strengthening the US-Japan alliance, while on the other hand, it would spend certain portion of its budget for not substantially important to protect Japanese assets. The final decision was made at the top of the political level. The Prime Minister has ordered that SSA should be included in the Basic Space Plan which defines mid-term space policy guidelines. MoD has begun working on developing deep space radar and telescope in Yamaguchi Prefecture for building SSA capabilities in cooperation with JAXA. SSA was also included in the National Defense Program Guidelines, which was adopted in 2018 (Ministry of Defense 2018).

The third priority is the early warning satellite system. Japanese government made a decision to construct missile defense system in cooperation with the United States when the Taepodong flew over Japanese territory in 1998. Furthermore, two Hwasong-12 missiles flew over Hokkaido and splashed into Pacific Ocean in 2017. These incidents made Japanese security policy community as well as the nation as a whole recognized that Japan is under serious threat, and something has to be done within the limit of the Constitution. Thus, together with the development of IGS, it became imperative to build missile defense capabilities. Japanese Theater Missile Defense System has constructed with four Aegis frigates and PAC-3 surface-to-air missiles, and there will be addition of two batteries of Aegis Ashore in early 2020s. However, Japan lacked early warning satellite system to detect missile launch. Currently, Japanese Missile Defense System entirely depends on the United States for early warning signal intelligence, but it has some problems.

In 2009, North Korean regime prepared to test its launcher, and Japanese SDF prepared to intercept if it falls on its territory. The launch itself was not successful and there was no harm in Japan, but the SDF ground-based radar has misinterpreted signals from Korean Peninsula and sent false alarm. Contrary in April 2012, when North Korea failed again to launch, Japanese government did not issue warning for the people living in the flight path because it wanted to double check if the early warning signal was not false alarm. The government was heavily criticized for both incidents and it was considered that the failures occurred due to the lack of early warning intelligence. As a result, there was a strong argument for having early warning satellite of its own would improve the detection capability and verification of the United States' early warning signal. Although MoD understood the importance of having early warning satellites, it is still reluctant to move forward because of the cost of developing these satellites. The MoD decided to develop Infrared sensors which will be mounted on Quasi-Zenith Satellite in Geostationary Orbit, but it is only for R&D purpose. There is no decision to develop operational early warning satellite yet.

---

## **JAXA's View on Space Security**

For many years, JAXA (formerly NASDA and ISAS) were prohibited to develop satellite or launcher technology explicitly aiming to improve military capability. However, space technology in general is dual-use technology, which does not

discriminate military and civilian use. There has been always suspicion that JAXA would have a hidden agenda to develop space technology for military purpose, despite the 1969 Diet Resolution. In order to eradicate the suspicion, JAXA had to emphasize its programs were designed, developed, operated, and used exclusively peaceful purpose. As a result, JAXA has averted anything that relates to security issues.

Thus, even after the Chinese ASAT test became public, JAXA was reluctant to call this issue as “space security” issue; but instead, it preferred to use the term “long-term sustainability of space environment.” In other words, JAXA wanted to frame the issue of space security within the issue of space debris regardless of whether the debris was created intentionally or not.

However, given the rapid increase of debris population especially in Low Earth Orbit, JAXA became concerned about the risk of collision with debris. The JAXA’s safety analysis procedure now contains the risk assessment of debris collision probability. Nevertheless, JAXA, as an R&D agency, demonstrated its interest not in the development of international regulation or rule of the road but in the development of new technology for debris removal. JAXA is increasing its budget allocation for the study of Active Debris Removal (ADR) technology. In 2020, JAXA concluded a commercial partnership program with Astroscale, commercial ADR venture, for experimental operation for debris removal.

The problem here is that any technology of ADR has possibility to be perceived as space weapon development, and also there are many political, economic, and legal problems on ADR technology even if JAXA would successfully develop one. JAXA’s legal department has been working on the possible interpretation of Outer Space Treaty and other space-related international agreements but has not taken any initiative to provide legal framework for debris removal activities.

---

## Japanese Reaction to the Code of Conduct

After the ASAT test by China, the global space community has moved toward establishing a general rule to prevent similar action which created large number of debris. In April 2007, the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) has adopted Space Debris Mitigation Guidelines, based on the Inter-Agency Space Debris Coordination Committee (IADC) Space Debris Mitigation Guidelines, which was published in 2002. Although these guidelines are not legally binding documents, they set up an ethical and social benchmark on what should be done to secure the safety of space environment. Furthermore, the delegates of European Union (EU) in the Conference on Disarmament (CD) in Geneva submitted Code of Conduct for Outer Space Activities. This document took a step further to set up norms of behavior of spacefaring states to protect space environment and prevent intentional as well as unintentional creation of space debris.

Since most of Japanese spacecrafts were R&D-oriented (not operational) ones, Japanese space community paid little attention to the risks of orbital environment. The risks of colliding with space debris or being targeted from hostile parties were

considered minimum because Japanese spacecrafts were not in military or public operations. In other words, the damages of losing these satellites were not important since the objectives of developing these spacecrafts were to test and demonstrate Japanese engineering capability.

Japan did not make an explicit action when the European Union proposed the Code of Conduct. Not only because Japan has not been ready yet to engage in the negotiation with the EU but also because the United States, Japanese major ally, did not express its position against the Code. Japanese government was well aware of the US national space policy which was published in 2006 during the Bush Jr. administration which explicitly rejected any international agreement that binds the freedom of American space activities. Although the Code assumed voluntary participation, the commitment to the Code would make the US space policy more constrained.

For Japan, the Code seems to be very suitable for the world after the 2007 ASAT test. Its voluntary nature would be essential for inviting as many nations as possible. Initially, the EU intended to make the Code a voluntary one in order to include spacefaring countries (the United States under Bush Administration in particular). But since the United States under Obama Administration preferred to establish international platform for negotiation based on the Code of Conduct, the dividing line emerged between Western countries (EU, the United States, Japan, and Australia) and China and Russia. By avoiding the division among spacefaring countries and making the Code as international norm, the voluntary nature of the Code is utterly important. Of course, it would be much effective if the Code is legally binding, but there is a trade-off. In order to include the countries such as China and Russia, it should be based on voluntary participation, at least in the beginning (Suzuki 2012c).

The most important clause in the Code of Conduct from Japanese point of view is the Clause 4.3, which states that “when executing maneuvers of space objects in outer space, for example to supply space stations, repair space objects, mitigate debris, or reposition space objects, the Subscribing States confirm their intention to take all reasonable measures to minimize the risks of collision.” This allows Japan to invest in the development of the technologies to remove space debris. JAXA in particular is very interested in developing debris mitigation and removal technology, but it is well-known that the removal technology can be used as space weapons. Thus, it is extremely important that the Code explicitly allows debris removal activities with good intention.

These interpretation underlines that Japanese perspective on the Code is based on its diplomatic and technological concerns, not on its military and security needs. Since MoD is not engaged in the process of decision-making for the Code, it would be difficult to assume that Japan would commit to the Code for security purposes. Although Japan expressed its interest to participate in the process of negotiation for drafting the International Code of Conduct, its objective is not purely driven by the needs for securing healthy environment for space activities. Rather, its objective is driven by the interest of JAXA and MoFA.

Currently, the negotiation on the Code of Conduct has completely stalled and it is impossible to foresee that there will be consensus to adopt the Code as international standard. Nevertheless, it is important for Japan and any spacefaring nations to have

international rules to govern increasingly crowded orbital environment. There are new states starting to launch their own satellites, and numerous constellation businesses are deploying thousands of satellites in already crowded orbits. The security and safety of orbital traffic is the primary importance of space security. Japan is willing to participate in any discussion for setting up rules of the road, but the political climate, especially that of US-China relationship, might not provide opportunity to even put the Code or any proposal for international rule-making on the negotiating table.

---

## Conclusion

Japanese perspective on space security has begun with a very unique setting. The 1969 Diet Resolution has put heavy constraints on its space activities, and long and enduring interpretation of “non-military” approach has refrained Japan from anything related to security. However, the 1998 Taepodong launch and subsequent reform of space policy eventually created Basic Space Law in 2008.

Although the new legal framework provides opportunity for Japan to play much bigger role in the field of space security, it seems that Japan is still taking steps cautiously. It is largely because the history and culture of Japanese space activities. The understanding of “exclusively peaceful purpose” as “non-military” nature of space has been long and persistent not only among the people in space community but also the people working in the security field. The Ministry of Defense and Self-Defense Forces do not consider themselves as the actor in space policy making, and they refrained from investing in space because they have constructed Japanese defense system without relying on space assets. Similarly, JAXA is reluctant to take security programs as its central mission. Under severe budgetary constraints, JAXA had to give up some of its pet projects for the sake of security program. Thus, it has resisted changing its status as civilian R&D agency.

Nevertheless, the security environment as well as the role of Japan is changing. On the one hand, the emergence of China as military superpower and the territorial dispute over Senkaku/Diaoyu Islands urge Japan to improve its surveillance capability and space-based infrastructure for SDF operations in the West Pacific and East China Sea. Furthermore, the successful launch of North Korean missiles over Japan increased awareness for building robust Missile Defense System. Japan can no longer have a luxury to stay away from the discussion on the space for security purposes.

On the other hand, increasing number of countries in Asia-Pacific region began using space systems as their national infrastructure, which provides indispensable services to their socioeconomic activities. Japan as one of the leading spacefaring nations in this region is taking a leadership to formulate regional space cooperation framework which includes a forum to discuss space security. The Ministry of Foreign Affairs took initiatives with Australia to hold a workshop within the ASEAN Regional Forum and APRSAF. These initiatives cannot be capitalized if Japan would not play active role for securing space environment.

Japanese space policy towards space security – both national and international security through space and security of space environment – is gradually changing

thanks to the Basic Space Law and changing security environment. There has been strong political intervention from Prime Minister to focus on SSA and missile defense which enabled Japan to participate in global SSA networks. The National Defense Program Guideline, for the first time, took up space as important domain to maintain superiority against other countries. These changes are now shifting the mindsets of MoD and JAXA, two most important but reluctant agencies for space security. Since the negotiation on the Code of Conduct is stalled and there will be no international consensus on the governance rules in space for a foreseeable future, Japan needs to develop its own plan and strategy to maintain space capabilities for itself and its allies. It is unthinkable in these days that military operations can be conducted without space infrastructure, and Japanese investment in space security would improve not only the survivability of space system for Japan but also for the allied countries.

---

## References

- Aoki S (2008) Japanese perspective on space security. In: Logsdon J, Moltz JC (eds) *Collective security in space: Asian perspective*. The Elliot School of International Affairs, The George Washington University, Washington, DC, pp 47–66
- Aoki S (2009) Current status and recent developments in Japan's National Space Law and its relevance to Pacific Rim space law and activities. *J Space Law* 36(2):335–364
- Consultation Group for National Strategy for Space (2005) *Toward a construction of new institutions for space development and utilization*. Liberal Democratic Party, Tokyo
- Hagt E (2007) China's ASAT test: strategic response. *China Secur* 3(1):31–51
- Kato K (1985) Government official statement. Budget Committee, House of Representatives, Feb 6, 1985
- Matsuura S (2004) *Kokusan rokketo wa naze ochirunoka (Why do Japanese launchers fail?)*. Nikkei BP Publishers, Tokyo
- Ministry of Defense (2018) *Heisei 31 Nendo ikou ni kakaru boueikeikaku no taikou ni Tsuite (National Defense Program Guidelines after 2019)*. Ministry of Defense. Retrieved from <http://www.mod.go.jp/j/approach/agenda/guideline/2019/pdf/20181218.pdf>
- Sunohara T (2005) *Tanjo kokusan supai eisei (The birth of national spy satellites)*. Nikkei BP Publishers, Tokyo
- Suzuki K (2005) Administrative reforms and policy logics of Japanese space policy. *Space Policy* 22(1):11–19
- Suzuki K (2006) Adopting the European model: Japanese experience in implementing a public–private partnership in the space program. Paper presented to the Council for European studies, Fifteenth biennial international conference, Chicago, Mar 31, 2006
- Suzuki K (2007a) Transforming Japan's space policy-making. *Space Policy* 23(2):73–80
- Suzuki K (2007b) Space: Japan's new security agenda. RIPS policy perspectives no. 5. Research Institute for Peace and Security, Tokyo
- Suzuki K (2012a) The leadership competition between Japan and China in the East Asian context. In: Morris L, Cox KJ (eds) *International cooperation for the development of space*. Aerospace Technology Working Group, Charleston, pp 243–259
- Suzuki K (2012b) Japan, space security and code of conduct. In: Lele A (ed) *Decoding the international code of conduct for outer space activities*. Institute for Defence Studies and Analyses, New Delhi, pp 94–96
- Suzuki K (2012c) Space code of conduct: a Japanese perspective. Analysis, Observer Research Foundation, July 25, 2012



Ajey Lele

## Contents

Introduction .....	572
India's Space Architecture .....	572
Space and National Power .....	577
Space for National Security .....	579
Military Specific Space Systems .....	581
India's ASAT Test (Lele 2019) .....	583
Conclusion .....	586
References .....	587

## Abstract

India could be said to have begun its space program during early 1960s by undertaking launching of sounding rockets. A structured approach towards evolving the space agenda for the nation could be said to have begun with the establishment of the Indian Space Research Organisation (ISRO) on August 15, 1969. The prime objective of ISRO is to develop space technologies to cater for various societal needs. Subsequently, the Department of Space (DOS) and the Space Commission were set up in 1972 which oversee planning and implementation of India space agenda. India launched its first satellite during 1975 and earned the space-faring nation status during 1980. Over the years ISRO's program has matured significantly and at present Indian space program is regarded as one of the important space programs in the world. From launching small satellites to undertaking a successful mission to Moon and Mars, India has excelled in almost all areas of space experimentations. India is also proposing to undertake its first human space mission by 2022. India is a nuclear weapon state and has made significant investments towards establishing its military

A. Lele (✉)

Institute for Defence Studies and Analyses, New Delhi, India

e-mail: [ajey.lele@gmail.com](mailto:ajey.lele@gmail.com)

architecture owing to its strategic needs. Space technologies are finding increasing relevance towards strengthening this architecture, essentially as a force multiplier. This chapter analyzes various significant aspects of India's space program.

---

## Introduction

The word "strategic," broadly gets identified as long-term and is mostly associated with the broad purposes and interests of an organization on enduring basis. The progression of strategic planning, generally involves establishing the definite purpose behind planning for a particular mission, the strategy for achieving the desired objective, and various processes involved towards that. The processes involve setting up of the priorities and allocation of resources accordingly. This chapter undertakes a strategic overview of India's space program. For long, the word strategic has established semblance to the military domain and gets often used linking to the realization of overall or long-term military policies and strategies. This chapter also specifically critically focuses on these aspects of India's space program too.

---

## India's Space Architecture

India launched its first sounding rocket on November 21, 1963. This launch took place from a location called Thumba in the southern parts of India. A church building at a place called Thumba village (in the Kerala province which is at the southern tip of Indian peninsula) is the place of birth of India's space program. This particular location was selected since the geomagnetic equator passes through Thumba and the church was selected because it was the only properly constructed building in that village (Das 2007). The sounding rocket launch was assisted by the National Aeronautics and Space Administration (NASA), which provided Nike-Apache rocket along with other required equipment. These were early days and India had limitations in regard to both financial and technological resources. During last five to six decades India has made a significant progress in the space domain and has also successfully conducted missions in deep space, to Moon and Mars.

During 1962, Indian government established Indian National Committee for Space Research (INCOSPAR). Subsequently, during 1969 INCOSPAR was superseded and Indian Space Research Organisation (ISRO) was established. Presently, this organization is the torchbearer of India space program and has brought many laurels to the country by undertaking various successful programs. In the changing world ISRO did realize the need for opening up their expertise for business. This led to the institution of Antrix Corporation Limited (ANTRIX) during 1992 a government of India Company. Both ISRO and ANTRIX are under the administrative

control of Department of Space (DOS) which got established during 1972. At the same time a space commission was also setup. The department of space and the space commission directly reports to the Prime Minister of India. Few public sector organizations like the Hindustan Aeronautics Limited (HAL) also play an important role towards assisting ISRO's various programs. The private industry also plays its role towards assisting ISRO in various projects. However, their involvement is more at subsystem level. India is under the process of establishing a full-grown eco system for private space industry. Defence Research and Development Organisation (DRDO) also plays some role essentially assisting India's defense establishment in the area of space.

Two scientists deserve a credit for conceptualizing and executing India's space vision in the early years. They are Dr Vikram Sarabhai (12 August 1919–30 December 1971) and Prof Satish Dhawan (25 September 1920–3 January 2002). It was Dr Sarabhai who gave the initial vision which was implemented and expended upon by Prof Dhawan. In simple terms, the articulated vision then was "to use space for socioeconomic development" which continues to remain relevant in the twenty-first century too.

India launched its first satellite in 1975 with assistance from the erstwhile USSR. Within 5 years after the launch of first satellite with the outside assistance, India became a spacefaring state during the 1980 by launching made-in-India satellite with the Indian rocket. Since then, India has made significant progress in the space domain and today India has earned a reputation of a committed and serious space player. Till date India has sent a range of satellites to different orbits. However, particularly to launch satellites into the geostationary Earth orbit (GEO) India is required to take the assistance from other agencies. This dependence is seen reducing by 2018 with India successfully developing a launch vehicle to send heavy (say 4–6-t category) satellites to GEO.

ISRO has come a long way from the Sounding Rockets (1963) to having capability launch heavy satellites with geostationary satellite launch vehicle (GSLV) Mark III (2018). Initially, ISRO began with Satellite Launch Vehicle-3 (SLV-3) program as India's first experimental satellite launch vehicle. India became the sixth spacefaring state in the world on July 18, 1980 when Rohini, a 40-kg satellite was placed in the Low Earth Orbit (LEO) by SLV-3. The successful culmination of the SLV-3 project showed the way for various advanced future launch vehicle projects. The next vehicle for ISRO was the Augmented Satellite Launch Vehicle (ASLV), which was followed by the Polar Satellite Launch Vehicle (PSLV) and the Geosynchronous Satellite Launch Vehicle (GSLV).

The Augmented Satellite Launch Vehicle (ASLV) Program was designed to augment the payload capacity to 150 kg, thrice that of SLV-3, for Low Earth Orbits (LEO). While building upon the experience gained from the SLV-3 missions, ASLV proved to be a low-cost intermediate vehicle to demonstrate and validate critical technologies for the future launch vehicle development projects like strap-on technology, inertial navigation, heat shield, vertical integration, and closed-loop guidance.



Polar Satellite Launch Vehicle (PSLV) is the third generation launch vehicle of India. It is the first Indian launch vehicle to be equipped with liquid stages. The PSLV-C45 mission on April 01, 2019 was its 47th mission and the PSLV rocket has witnessed only two failures till date since its first successful launch in October 1994. The rocket is fondly known as the most reliable workhorse of ISRO. Till April 01, 2019, PSLV has launched 46 Indian satellites, 10 satellites built by students from Indian Universities and 297 international customer satellites. Even India has used this rocket for its first mission to moon, the Chandrayaan-1 in 2008 and for the Mars Orbiter Mission (MOM) in 2013.

The PSLV mission configuration constitutes four stages using solid and liquid propulsion systems alternately. The first stage carries solid propellant, and the second stage uses the indigenously developed Vikas Engine which carries liquid propellant. The third stage is a solid stage and the fourth stage is a liquid stage with a twin-engine configuration. PSLV can take up to 1,850 kg of payload to Sun-Synchronous Polar Orbits of 600 km altitude. It has also carried payload of 1,425 kg to Sub GTO. Due to its unmatched reliability, PSLV has also been used to launch various satellites into Geosynchronous and Geostationary orbits, like satellites from the IRNSS (NAVIC) constellation. There are different variants of PSLV depending on the nature of the mission and the weight of the payload to be carried. Four to six ground-lit strap-on boosters are added (attached) to the rocket based on the requirement.

The flexibility of the PSLV system is amazing. This one rocket which ISRO is using for multiple orbit launches in a single mission. Also, ISRO has successfully started using the fourth stage of the rocket for carrying out scientific experiments. It is important to take note of two new features of the PSLV system which ISRO has started experimenting with since 2015. One, single mission undertaking two/three orbit launches and two, using the fourth stage of the rocket as a platform for experimentation. Developing capabilities to launch satellites into different orbits in a single mission gives ISRO more flexibility to manage their commercial interests. ISRO has developed and aptly demonstrated its capability to launch multiple satellites in a single mission. The PSLV-C37 mission on February 15, 2017 created a world record by successfully launching 104 satellites in single mission (during May 1999, with PSLV-C2 mission ISRO had launched more than one satellite in a single mission). Now, this added capability of launching satellites in different orbits in one mission could attract more international customers.

Another less debated but a significant feature is about ISRO demonstrating its capability to convert the fourth stage of the rocket into an experimentation platform. Space is a medium where scientific and strategic communities are keen to undertake various experimentations for many decades for various purposes. Mainly such experiments are important since they are carried out in (almost) zero-gravity atmosphere. Such experiments are useful also from the point of view of learning for the futuristic space (both manned and unmanned) missions.

The International Space Station (ISS), a station with 16 member states, is known to serve as a microgravity and space environment research laboratory. This station has been inhabited continuously since the year 2000. Here the astronauts from the

member states are conducting experiments in biology, physics, astronomy, meteorology, and few other fields. Now, China is also going to establish its own space station in near future. Against the backdrop of this, India's efforts to conduct experiments in space could look infinitesimal. ISRO is expanding the fourth stage of the PSLV, as a laboratory for conduct of experiments. Here there is no human element involved towards the conduct of such experiments, but still that in no respect reduces the relevance of such unique experimentation. The maturing of the UAV technology has demonstrated that to a certain extent and for specific purposes an alternative on a manned flying platform is feasible and available. Today, India may not have its own space station, but the innovation of ISRO indicates that developing such techniques (extremely cost effective) of converting the fourth stage of the rocket into a laboratory could definitely offer India a moderate alternative to the space station.

For many years, the major success achieved by ISRO towards developing a reliable launch vehicle for LEO to carry around 2-t verity satellites could not be repeated for geostationary orbit. ISRO struggled for many years to fully establish its Geosynchronous Satellite Launch Vehicle (GSLV) program. There has been significant amount of dependence of ISRO on outside agencies for launching 4–6-t verity of satellites in the geostationary orbit. The first launch of GSLV mission was launched during April 2001 with a payload mass of 1,540 kg. Till date, the maximum lift-off mass of 3,423 kg has been put in Geosynchronous Transfer Orbit (GTO, GSLV Mk III-D2/GSAT-29 Mission, November 14, 2018) by ISRO. GSLV is a three-stage system with solid, liquid, and cryogenic stage.

The major challenge which India had faced was about mastering the art of cryogenic technology. In fact, a Cryogenic Study Team was set up at ISRO as early as 1982; however, this idea got neglected. Finally, around 1990s when the need arose, India got in the technology transfer agreement with Soviet Union/Russia. However, this arrangement could not work owing to the international (read the US) pressure. The USA and its partners in the then 18-member Missile Technology Control Regime (MTCR) contend that the Indo-Russian deal is inconsistent with the MTCR, which was set up in 1987 to prevent the transfer of missile technology to non-member countries. The Russian republic was not a signatory to the accord but has agreed in principle to abide by its guidelines since it had applied for what is called "adherent" status (Russia joined MTCR during 1995). Also, the National Defense Authorization Act of the USA (1991) had provisions for penalties for such transfers. Thus, both Glavkosmos of Russia and the ISRO would have got blacklisted if the deal had gone through. At the hindsight it could be said that the Russian leadership then (Boris Yeltsin) capitulated to the US pressure and the transfer of cryogenic engine technology deal was cancelled. Finally, Russia was allowed to supply only seven cryogenic engines to India.

Broadly, it could be argued that Cryogenic engines and associated technological knowledge has almost no relevance for missile launches in war. This is because the procedure of fueling this system requires few months' time. Even missile system with liquid fuel stages are not preferable since the crucial time gets wasted and particularly the process of fueling requires to be undertaken at the launch site (almost

close to the battlefield). However, the major powers appear to have taken the advantage of MTRC provisions by undertaking selective (mis)interpretation. Finally, India decided to develop these engines on its own, but it took considerable amount of time for the development. However, the development of the indigenous cryogenic engine took much time (almost three decades) and only on June 05, 2017 GSLV Mk III-D1 launched GSAT-19, a 3,136 kg bird (ISRO 2017a; Chengappa 2013; Krishnan Simha 2013). For all these years the basic limitation of India's space program has been its inability to develop a cryogenic engine, but now that challenge has been overcome.

Keeping an eye on the future commercial market for launch of small satellites, ISRO is also developing a Small Satellite Launch Vehicle (or SSLV) for an approximate payload capacity of 500 kg and expected to undertake the first flight by mid of 2019.

Satellite technology development is a complicated task. Also, satellites once launched are required to survive in space for number of years. Hence, their manufacturing requires components and systems with very high reliability. India understood the need of outside assistance in this field, if they have to make progress. During its formative years India took significant foreign inputs to build threshold capabilities in complex systems. Initially, ISRO took assistance from developed space powers to build different kinds of payloads for sounding rocket experiments (Baskaran 2001). Over the years India has acquired good capability to build very complex and world-class satellites for remote sensing, weather, and communications. India has also developed good capability in other sectors like navigation and various categories of small satellites.

The first important structure established by India towards working on satellite technology was the Experimental Satellite Communication Earth Station (ESCES) at the city of Ahmedabad in 1967. During 1970s, Indian engineers got trained in France. ISRO started developing sensors for airborne remote-sensing surveys and processing of imageries provided by NASA. Subsequently, few satellites were built and launched. This was basically an experimental phase for the scientists. This was followed by the conceptualization of two major projects which actually would be viewed as the beginning of a very systematic and organized space agenda. The socioeconomic focus articulated earlier was evident. These two satellite programs included: the Indian Remote Sensing Satellite system (IRS) and the Indian National Satellite system (INSAT), for commercial operations. Probably, ISRO was confident about their capabilities in the remote sensing arena but not that much about the telecommunication field which incidentally was also a high priority area. Hence, after a realistic appraisal of its capabilities, it was decided that the IRS-1 series would be indigenously built and the INSAT-1 series would be brought from abroad. It was also decided that the INSAT-2 series would be built indigenously. There were reasons behind these decisions. As INSATs were communications satellites, they were more complex and ISRO needed longer development time. INSAT is a unique experiment which has not been replicated elsewhere. During 1977, ISRO defined INSAT as a multipurpose system consisting of telecommunication, meteorological, and TV broadcasting elements. It was the world's first geo-stationary satellite system

to combine these three elements (Baskaran 2001). That was the period when India was not in a position to afford specific satellites for specific purposes, hence decided to have one satellite which could be multipurpose.

Today, India has a technologically mature remote sensing satellite program. There is an array of Indian Earth observation (EO) satellites with imaging capabilities in visible, infrared, thermal, and microwave regions of the electromagnetic spectrum, including hyper-spectral sensors. The imaging sensors have been providing spatial resolution ranging from 1 km to less than 1 m. India has launched various other satellites for communication, education, meteorology, astronomy, and navigation purposes. India's own navigational system is a regional system with seven satellites. All satellites have already been placed in orbit and the system is expected to become fully operational in the near future. A ground network of several nodes for data gathering has been set up under various collaborative mechanisms to establish a global chain of command and control for its space assets.

India has also put in place a well-articulated Deep Space agenda. India's first Moon mission, Chandrayaan-1 (2008–2009), was successful. This mission was instrumental towards the discovery of water on the Moon. The second lunar mission encountered delays, given uncertainties in Russia, which was assisting India with a rover and lander system for this mission. Presently, India is undertaking this mission with an indigenously designed and developed rover and lander system and is expected to get launched during the second half of 2019. India's first mission to Mars, Mars Orbiter Mission (MOM), was also successful. MOM which was designed for 6 months of stay, has been orbiting Mars since September 2014. India is the only country in the world till date which had successfully entered into the Martian orbit in the first attempt. India proposes to undertake its first human space mission by 2022.

There has been some amount of criticism with respect to India, as a developing state for having made investments in the programs like Moon and Mars. However, one of the chief architects of India's space program Prof S Dhawan (1996) had argued to the effect that, "it is moral to planets and stars in spite of having hunger, poverty and misery on earth because various programs which explore the planets enhance human's capacity to face the unknown and severe to survive in any environment. Humans reach to space for solving problems on earth" (In a lecture delivered at Astronomical society of India at the city of Bangalore on September 6, 1996).

---

## Space and National Power

Normally, it has been observed that space programs of various states are born out of their ballistic missile programs. However, that is not the case with India. Since initiation of its space program it has been witnessed that India is having a focused attention on developing and using space for societal purposes. Satellite systems used for the purposes like meteorology, remote sensing, and communications were seen exclusively used for the purposes like weather forecasting, TV, education, resources mapping, and medicine.

It is also important to factor in the strategic milieu at global level during the formative years of India's space program. It was a period of Cold War and mostly the world was divided into two power blocks. India was one of the few countries which were not under the influence of any superpower. Since independence (1947), the then political leadership had taken significant amount of interest towards investing in science and technology. Political leadership, policy makers, and scientific community were found working in unison. It was a considered view that if India has to progress, then investments in science and technology are a must. There is no evidence to show that Indian state had any interest to use their investments in technology as a tool to display power. At the same time, it needs to be acknowledged that immediately after independence both from economic and strategic perspective India was not in a position to project power.

Satellite technology is inherently dual-use in nature and in a limited way could even be used for military requirement by any power which has control over it. During Cold War period, space technology could be seen as a currency of that of force (technology) projection. Subsequently, the 1991 Gulf War ended up showcasing the importance of space technologies in the warfare. Actually, this war was an eye-catcher for many states in respect of utility of space systems in the warfare and India was no exception. At the same time, it is important to put in context the level of proficiency achieved by India in the space domain then.

ISRO was established on August 15, 1969, while a month before that on July 20, 1969, Apollo 11 had already landed on the moon. On August 29, 1991, India has launched IRS 1-B, a 975 kg satellite from the Baikanur Cosmodrome Kazakhstan using Launch vehicle Vostok. This remote sensing satellite had three solid state Push Broom Cameras with resolutions ranging from 72.5 to 36.25 m. During the 1991 Gulf War, the USA and allied forces had range of remote sensing satellites like SPOT (France) with 10 m resolution and other satellites KH 11 (Block I and Block II) and few Landsat series satellites (Marcia and Smith 1991). During the year 1991, NASA had undertaken six human missions to space by using the Space Shuttles (models used Atlantis, Discovery, and Columbia) while India yet to undertake its first human mission to space (could happen by 2022). The USA had fully operational GPS satellite navigational system during the 1991 Gulf War and India is yet to (by April 2019) operationalize its regional satellite navigational system. All this indicated that the use of space technologies during 1991 Gulf War could have been much learn for countries like India; however, technologically India was nowhere close to the capabilities of the allied forces in the space domain. More importantly Indian policy makers were fully aware that any military investments in space from their side should be threat specific and there is no requirement to raise the ante just because the demonstration of technologies have happened some other theatre of war.

It is well understood that national power and aspects of national security is not only about military influence but is also about political and economic influence. The core of national power is also about national performance and management of natural resources. The realization of national performance involves ensuring socioeconomic development. Under such framework, there has been major and continuing focus by India towards using space for communication, meteorology,

education, tele-medicine, disaster management, linking of cities and villages, scientific research, and navigation. One of the major utilities of the satellites for India has been in the field of meteorology essentially because India is an agricultural economy and timely weather information is critical. Also, remote sensing satellites have much of utility for resources planning and management. Such satellites also provide useful information on range of issues from forest cover to inputs for river and ground water management. Education and telemedicine are two important areas where India is known to be using space technologies very effectively. In addition, various communication satellites are catering for the needs of television broadcasting and other sectors. India is also looking at space as a tool for foreign policy. On May 05, 2017, India has launched a communication satellite (GSAT-9) which is providing assistance to the South Asian states, namely, Bangladesh, Afghanistan, Nepal, Bhutan, Sri Lanka, and Maldives. Space is an important part of India's various multilateral and bilateral arrangements for many years.

Realizing the importance of commercial facets of space sector, way bank during 1982 India had established the commercial arm of ISRO called ANTRIX for promoting products, services, and technologies developed by ISRO. However, India has not been able to make a significant dent to global commercial space sector, yet. One of the key commercial focuses for ISRO has been to provide satellite launching services to the foreign customers. ISRO could be said to have a specialization in the field of small satellites (mini, micro, and nano) launching. However, for all these years ISRO has launched just about 300 satellites for the international customer (till Apr 2019, it had launched 297 satellites). The market size of launch services currently is about \$5.5–6 billion globally and India has some 7% of this market share. However, ISRO is keen to increase its overall market share significantly. Currently, the revenue of ANTRIX is Rs 20 billion (20 billion INR is equal to 288,400,000 USD) and the company expects to double it within next 5 years (*Sun*, September 092018). ISRO is also working towards privatizing its launch services. As the name suggests, it is but obvious that the main business of ISRO is not business but to undertake research and development. Hence, presently ISRO is working towards commercializing the PSLV launching services. It is expected that as and when the small satellite launch vehicle becomes operational, it would also be fully commercialized. Apart from launch services, ANTRIX also provides other services like data, imagery, and ground infrastructure construction.

---

## Space for National Security

It is important to highlight broad security challenges which India is facing before identifying the military-related investments made by India in the military domain. India has two advisories in the region, namely, China and Pakistan with whom conventional wars have been fought in past. Basically, the differences are owing to the unresolved boundary disputes with these states. They exist since India got independence from the British power during 1947. China and India share a border of over 4,000 km, with nearly all of it founded on colonial-era settlements and

surveys and much of it still under dispute. China has certain claims over Indian Territory and India has some on the territory under the Chinese control. India shares more than 3,300 km land border with Pakistan and have some unresolved border issues. Kashmir dispute is the key security challenge which India is facing presently. Owing to this problem, continuous bloodshed is happening in the region for last few decades. One of the recent confrontations witnessed between India and China was the crisis of Doklam from June to August 2017. However, luckily in the last 40 years, not a single bullet has been fired because of the border issue. There are few other differences amongst these three states, like water issues and China's new economic/security project called Belt and Road (BRI) initiative. India has a major objection to the part of the BRI project called the CPEC, the China–Pakistan Economic Corridor. Here, China is trying to advance this project without concerns for India's unresolved border problems with Pakistan.

Essentially, India could be said to have saddled in a typical security scenario with unresolved border issues for more than seven decades. At the same time, India also faces few internal security challenges owing to both inter and intra state security problems. India's paramilitary forces play an important role to address such challenges and it is important to note that they also require (and want) assistance from the satellite systems.

India has fought four wars with neighbors since independence. British government during 1947 divided the then united India which they were ruling into two differ states: one remained as India and a portion of India was declared as Pakistan. Immediately, after that the first war was fought between India and Pakistan over the Kashmir issue. Owing to the differences with China on boundary issue, a war was fought during 1962. Subsequently, India and Pakistan have fought two more wars during 1965 and 1971. The last conflict fought between these two powers in the Kargil conflict (May and July 1999), few consider this conflict as a half-war. Since Pakistan was not able to win any of the wars/conflicts against India for last few decades, they are found using Terrorism as a tool for possible conflict resolution (!).

China conducted its first nuclear test during 1964, and by 1967 they have also conducted their hydrogen bomb test. India and Pakistan became nuclear weapon states by 1998. All these three states have advanced missile programs and various types of missiles in their inventory. These states also have made investments into different category of missiles which could be launched from land, air, and submarine-based platforms. China has Nuclear Triad in place while India is almost there. Pakistan could take some more time to establish a Nuclear Triad. China and India have Intercontinental Ballistic Missiles (ICBMs) in their inventory. China has tested multiple independently targetable re-entry vehicle (MIRV) missiles while Pakistan is known to be developing this technology. China has developed hypersonic weapons and India is also known to have interest in MIRV and hypersonic technologies. Both China and India have Russian made S-400 Ballistic Missile Defence (BMD) systems. India is developing its own missile defense architecture.

India's strategic area of interest is not restricted to Pakistan-China. Geographically, India's location at the base of continental Asia along the Indian Ocean places the state at a vintage point in relation to maritime trade. India has a strong stake in the

security and stability of these waters since a large percentage of Asian oil and gas supplies is shipped through the Indian Ocean. (From the speech delivered by Mr. Pallaim Raju in the PC Lal Memorial Lecture on March 19, 2007, at New Delhi. Mr. Raju was then the minister of state for Defence in the government of India) As per the United Nations Department of Economic and Social Affairs (UN DESA 2017) report (UN DESA 2017), India has one of the largest diaspora populations in the world with over 15.6 million. A major part of Indian diaspora mainly constituting of unskilled or semiskilled workers is largely found employed in Middle East and African region. India feels responsible for security and safety of this population. India has conducted more than 30 evacuation operations across Africa, Asia, and Europe, including its largest-ever civilian airlift of 110,000 people from the Persian Gulf in 1990 (Constantino 2017). During 2015 in one of the major evacuation operations (Op Raahat) by sea, India evacuated 5,600 people, including 4,640 Indian nationals and 960 nationals from 41 countries, from Yemen (Ians 2015). Indian Air Force and Indian Navy have played a crucial role in these operations. For major natural disasters help of Indian armed forces is always sought. During 2004 Indian Ocean tsunami, particularly Indian Navy have played a major role towards search and rescue operations and had helped many affected countries. Even naval amphibious warfare vessels and landing craft were put in use. All these indicate that the role of the Indian armed forces is not restricted only towards guarding the state. Also, on various occasions Indian troops are deployed for contributing towards the United Nations peacekeeping missions. In conduct of all such operations space technologies have an important role.

Space technologies have an inherent dual use character. Obviously, various Indian satellite systems could be viewed to have some utility for the Indian armed forces. It is also important to note that modern-day warfare is about remaining ready to address various types of contests. Such tasks could involve remaining ready for conventional warfare, nuclear warfare, asymmetric warfare, and hybrid warfare. Modernizing the armed forces in terms of technology, weapon platforms, and weapon system is a dynamic process. Present day conceptualization of Revolution in Military Affairs (RMA) demands changes in doctrines to suit new technologies, equipment, and tactics. For a state like India, to bring radical changes in equipment and arms inventory is not possible essentially owing to financial issues. India is expected to follow a hybrid RMA approach were at any given point in time both old and new weapon systems and fighting platforms would be available. Investments in space would be from a point of view of a “force multiplier” to the existing military architecture.

---

## **Military Specific Space Systems**

So far India has launched few military specific satellites. Essentially, it is found that officially such satellite systems are identified more as systems with strategic utility than actually calling them as military satellites. India has been launching remote sensing satellites for many years. On October 22, 2001 ISRO had launched



a Technology Experiment Satellite (TES), weighing 1,108 kg in 572 km Sun Synchronous orbit. This satellite gets recognized as one of the first satellites launched for experimental as well as strategic purposes.

The first satellite exclusively claimed by the Indian establishment as a satellite for military purposes is the communications satellite (GSAT 7) launched for Indian Navy during 2013. This satellite is also known as Rukmini and has nearly 2,000 nm “footprint” over the Indian Ocean region and provides significant assistance to Indian Navy. Another communications satellite was launched during 2018 called GSAT-7A for Indian Air Force. This satellite is used to interlink ground radars, unmanned aerial vehicles (UAV) airbases, and Airborne Warning and Control System (AWACS).

During 2015, a communication satellite GSAT-6 got launched which has been also described as a system for strategic use. Owing to topographical challenges (India has various features from oceans, deserts, snow to thickly vegetated jungles), soldiers on many occasions encounter breaks in commutations. This geostationary satellite with S-Band antenna is used for gathering information over Indian mainland and very small handheld devices are used for data, video, or voice transfer.

It is expected that few more satellites would be launched to cater for the requirements of India army and other agencies. GSAT 7B is expected to be launched for Indian Army in near future. There are some proposals like development of GSAT 7D and 7E. But this is no official confirmation in this regard. Also, it is expected that some E/O satellites would be launched in the future.

India’s expertise in the remote-sensing arena is coming handy to establish a network of reconnaissance satellites. This activity could be said to have started with the TES launch during 2001. Now India has satellites with sub-meter resolution which essentially are dual-purpose satellites. India has also launched (with Israeli assistance) two Synthetic Aperture Radar (SAR) satellites called RISAT II (2009) and RISAT I (2011) essentially to address terrorism-related threats. Also, a Hyper-Spectral Imaging Satellite (HysIS) was launched during 2018. Following table provides details about Cartographic satellites:

Name of satellite	Launch date	Resolution	Remarks
<b>Cartosat-1</b>	5 May 2005	2.5 m	
<b>Cartosat-2</b>	10 Jan 2007	Less than 1 m	
<b>Cartosat-2A</b>	28 Apr 2008	80 cm	Perceived to be for the Indian armed forces
<b>Cartosat-2B</b>	12 Jul 2010	Less than 80 cm	
<b>Cartosat-2C</b>	22 Jun 2016	”	Used for weather mapping too
<b>Cartosat-2D</b>	15 Feb 2017	”	

(continued)

Name of satellite	Launch date	Resolution	Remarks
<b>Cartosat-2E</b>	23 Jun 2017	”	
<b>Cartosat-2F</b>	12 Jan 2018	Could be less than 50 cm	For mapping, enhance disaster monitoring & damage assessment

These satellites are proving very useful for the Indian Armed Forces. However, there is very less real-time data availability. Particularly, owing to cross-border terrorism, India is forced to have a continuous vigilance of its border. Existing space-based resources are not adequate to cater for various security challenges. India requires a major space-based surveillance network. As per the assessment carried out by experts, India would require a constellation of 24 small satellites in LEO for meeting ISR needs during times of crises. Also, this report identifies the need for a constellation of 40 satellites in LEO that provide Internet services for the military (Chandrashekar 2015).

In the field of navigation, India has developed an Indian Regional Navigation System (IRNSS/NavIC) (ISRO 2017a). The space segment of this system consists of the constellation of eight satellites: three satellites in suitable orbital slots in the geostationary orbit and the remaining four in geosynchronous orbits with the required inclination and equatorial crossings in two different planes. Currently, all these satellites have been positioned in their respective locations and the system is expected to become operational shortly.

NavIC is designed to provide accurate position information service (primary service area) to users in India and the region extending up to 1,500 km from its boundary. There is also an Extended Service Area covering more area. NavIC would provide two types of services: Standard Positioning Service (SPS) and Restricted Service (RS), which is an encrypted service provided only to the authorized users. This IRNSS System is expected to provide a position accuracy of better than 20 m in the primary service area. Possibly for military users the accuracy could be 10 m or less.

---

## India's ASAT Test (Lele 2019)

On March 27, India conducted Mission Shakti, an anti-satellite missile test. This was a technological mission carried out by the Defence Research and Development (DRDO). During this test, India targeted one of its own satellites with a ground-based missile. With this successful demonstration, India becomes the fourth country to test an ASAT after China, Russia, and the United States.

The satellite used in the mission was one of India's existing satellites, Microsat-R, operating in a low orbit about 300 km high. Such tests require an extremely high degree of precision and technical capability and, with the success of the test, India has demonstrated such capabilities. This test also demonstrates the maturation of India's missile defense program.

Looking at the types of missile interceptors being used for these tests broadly, it could be argued that such tests are the offshoot of ballistic missile defense programs of the respective nations.

ASAT testing is not a new phenomenon. During the Cold War period, the United States and former Soviet Union conducted a number of such tests. More recently there have been two ASAT tests. In January 2007 China conducted an ASAT test, the first such test conducted in the post-Cold War era. This test was followed by the US test in February 2008 when they destroyed an out-of-control intelligence satellite at an approximate altitude of 250 km.

These two tests and the test conducted by India were essentially hit-to-kill or direct ascent systems or a KKV (Kinetic Kill Vehicle) missions. Here the warhead of a missile is not an explosive but rather a piece of metal. This metal warhead hits the satellite and, owing to the impact velocity and the kinetic energy thus generated, the satellite is broken up. The Indian test used DRDO's Ballistic Missile Defence interceptor, which is a part of India's ongoing ballistic missile defense program. Reports indicate the test has generated at least 250–300 pieces of trackable debris. Such debris is expected to re-enter the atmosphere within next 1–2 months because of the low altitude of the satellite struck by the ASAT.

The 2007 Chinese test involved the destruction of an old weather satellite. This 750-kg satellite was orbiting at altitude of about 850 km. China used ground-based midcourse missile interception technology in that test. The problem with the Chinese test was that since it was conducted at higher altitudes, much of the debris created remains in orbit today. Moreover, it is even increasing in numbers as debris strikes each other or other objects in orbit. The US test a year later was conducted by using a modified Standard Missile-3 interceptor, essentially designed to counter short to intermediate-range ballistic missiles. This missile was launched from a ship-based platform. The debris created by this test re-entered, mostly within weeks of the test.

Looking at the types of missile interceptors being used for these tests broadly, it could be argued that such tests are the offshoot of ballistic missile defense programs of the respective nations. ASAT weapons of the KKV variety are useful only for hitting targets in low Earth orbit, up to about 2,000 km. DRDO is confident that they can hit a satellite by a ground-based interceptor up to a distance of 1,000 km. There is no authentic information available with regard to capabilities of countries like Russia, the USA, and China about the orbits they could reach with their missile interceptors. Some reports indicate that China is testing kinetic interceptors that can reach satellites in the geostationary orbit, 36,000 km high.

Over last two decades India has steadily and thoughtfully increased its investments in the space domain. At present, India has about 50 operational satellites in different orbits. Most of satellites are communications (19) and Earth observation (17). Obviously, India needs to ensure that their satellites are safe. India's space research organization has been working on satellite hardening technologies, while scientists and policymakers are trying to ensure that redundancy would be built-in in various systems as such. Possibly, owing to geostrategic compulsions, India's government felt the need to display the technological capabilities related to anti-satellite weapons.

One important geopolitical aspect of this test was that there was an official announcement of the test by Indian prime minister. This implies that India wants to be transparent in all activities it wants to undertake in space. Space security is an important issue for India and the highest level of decision-making structure is handling the issues concerning space.

There are differing opinions globally regarding the rationale behind this test. There is a need to situate Indian test in the overall security matrix of the region. India shares borders with China and Pakistan and there are some unresolved import border issues. Terrorism is a major challenge for the region. Unfortunately, no immediate solution to this problem appears to be in sight. All three nations are nuclear power states and have various missile systems in their inventory. The last classical war that this region witnessed was the 1971 war between India and Pakistan. At that time both the states were non-nuclear weapon states. India and Pakistan became nuclear weapon states by 1998. There have been various major security-related disagreements in the region over the years, but luckily no major war has broken out. Hence, there is a case to argue that nuclear deterrence has delivered.

In the missile domain, in spite of all these nations conducting various tests, no untoward incident has happened so far. India and Pakistan have a treaty that requires both nations to give advance warning to each other in respect of their proposed ballistic missile tests. This arrangement is working well.

In the space arena, China has put in place a major space program. India also has reasonable capabilities in the space arena. In a relative sense, Pakistan's investments are limited, but they have some sort of "space umbrella" from China. China demonstrated its ASAT capabilities more than a decade ago. The general notion that testing of military systems is destabilizing is found bit misplaced in this region. In fact, the acts of terrorism in the region have been more destabilizing than testing of any military systems. It is obvious that India's ASAT would be criticized by both of its adversaries, but there is a space for such noise in international politics. However, in the longer run India's ASAT testing is expected to emerge more as a stabilizing action for the region. Such a demonstration of technological capabilities is expected to deter potential adversaries.

More importantly, India's test is unlikely to increase the space debris problem. Experts had mentioned that there is no threat to the International Space Station since the Indian test took place well below the station's 400-km altitude. However, as per NASA's assessment some part of the debris had reached to the higher orbit, but many calculations show that there is very less probability of ISS coming in the impact zone. Also, since the debris created by the 2008 US test disappeared within days after the test, the same is expected to happen in this case.

Interestingly, the US Strategic Command chief General John E. Hyten has defended India before members of the Senate Armed Services Committee, saying that the country had tested the anti-satellite missile because it needed the capability to defend itself in space. The general called for international norms of behavior in space to curtail the dangerous debris issue (Sputnik News 2019).

Also, there is a need to take a note that India is the only state that has officially announced its ASAT testing. This announcement was made by none other than the

Indian Prime Minister Narendra Modi himself. Presently, India is in the grip of election fever. However, there is a need to look beyond domestic politics and assess the importance of the prime minister owing the test. With his announcement of this mission, it becomes clear that India wants to be transparent in all activities it wants to undertake in space. Space security is an important issue for India.

The possible weaponization of space is an issue of major concern for many nations, including India. Unfortunately, the space arena has very limited globally accepted multilateral treaty mechanisms, and such available mechanisms are mostly issue-centric and could not be viewed as all pervasive. For example, the 1967 Outer Space Treaty (OST) is basically about the banning of testing of weapons of mass destructions in outer space. For last decade or so, some efforts have been made to address this issue, such as the European Union and its International Code of Conduct.

India fully supports the formulation of universal and nondiscriminatory transparency and confidence-building measure, although such measures have limited relevance since they typically are not legally binding. Nonetheless, India believes such mechanisms have a useful complementary role and could become an “appetizer” for formulation of any future treaty. India has participated actively in the consultations called by the EU since 2012 to discuss a draft Code of Conduct for Outer Space Activities.

The possible weaponization of space is an issue of major concern for many nations, including India. Unfortunately, the space arena has very limited globally accepted multilateral treaty mechanisms.

Resolution 69/32, titled “No First Placement of Weapons on Outer Space” and adopted in the United Nations General Assembly on December 2, 2014, has the full support by India. However, India feels that there is a need to grow beyond such ideas and decide on a released and legally binding treaty. In this context, India is ready to give consideration to the revised PPWT (Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space Objects) presented by Russia and China in the Conference on Disarmament. There has been a total rejection of this proposal by some major powers. However, India is of the opinion that such ideas need to be discussed under the UN umbrella.

---

## Conclusion

India has made significant progress in the outer space area and has earned a global reputation for its professionalism. Since the inception of its space program, India has followed the policy of the use of space for socioeconomic development, and this agenda remains valid today. India is also keen to develop its space industry. ISRO has earned good reputation in the area of satellite launch market particularly in the small satellite sector and is keen to expand further. India is also effectively using space as tool for diplomacy.

India does not have a well-articulated Military Space Program but has launched some space assets for the Military. It is known that satellites provide various benefits,

but substantial vulnerabilities too, owing to both natural and man-made threats. Owing geopolitical realities, India needs to ensure that its assets in space are secure. Hence, to demonstrate that its defenses are ready, India has undertaken an ASAT test. It is expected that the way nuclear and missile deterrence has worked in the region, the ASAT deterrence would also deliver and weaponization of space would not happen.

India fully understands that space is an extremely important area for human survival and should not be tinkered with unnecessarily. Modern-day life is totally dependent on assets in space. India's growth story, scientific and economic, also involves the contributions made by its space agency and space industry. Today, space offers a major soft-power potential for India, and India believes that it is in nobody's interest to weaponize space. The need of the hour is to evolve a rule-based and transparent mechanism for protecting space.

---

## References

- Baskaran A (2001) Competence building in complex systems in the developing countries: the case of satellite building in India. *Technovation* 21:109–121
- Chandrashekar S (2015) Space, war & security— a strategy for India. National Institute of Advanced Studies, Indian Institute of Science Campus, Bengaluru, pp 6–8
- Chengappa R (2013) US blocks critical cryogenic deal, forces India to indigenise. *India Today Press*. <https://www.indiatoday.in/magazine/science-and-technology/story/19930815-us-blocks-critical-cryogenic-deal-forces-india-to-indigenise-811389-1993-08-15>. Accessed 10 Apr 2019
- Constantino X (2017) India's expatriate evacuation operations: bringing the diaspora home. *Carnegie India Press*. <https://carnegieindia.org/2017/01/04/india-s-expatriate-evacuation-operations-bringing-diaspora-home-pub-66573>. Accessed 03 June 2019
- Das SK (2007) *Touching lives: the little known triumph of the Indian space programme*. Penguin Books, New Delhi, p 1
- Ians (2015) India evacuates 4,640 nationals, 960 others from Yemen. *One India Press*. <https://www.oneindia.com/india/india-evacuates-4640-nationals-960-others-from-yemen-1711703.html>. Accessed 03 June 2019
- Indian Space Research Organisation (2017a) IRNSS programme. <https://www.isro.gov.in/irnss-programme>. Accessed 03 June 2019
- Indian Space Research Organisation (2017b) Launchers. <https://www.isro.gov.in/launchers/>. Accessed 10 Apr 2019
- Krishnan Simha R (2013) How India's cryogenic programme was wrecked. *Russia Beyond Press*. [https://www.rbth.com/blogs/2013/12/04/how\\_indias\\_cryogenic\\_programme\\_was\\_wrecked\\_31365](https://www.rbth.com/blogs/2013/12/04/how_indias_cryogenic_programme_was_wrecked_31365). Accessed 10 Apr 2019
- Lele A (2019) The implications of India's ASAT test. *The space review*. <http://www.thespacereview.com/article/3686/1>. Accessed 03 June 2019
- Marcia S, Simth (1991) *Congressional Research Service, The Library of Congress*
- Smith SM (1991) *Military and civilian satellites in support of allied forces in the Persian Gulf War. Congressional Research Service (CRS) report for the US Congress*
- Sputnik News (2019) India's ASAT justified, but space debris still a concern says Pentagon – report. *Press*. <https://sputniknews.com/asia/201904121074075266-pentagon-justifies-indian-asat/>. Accessed 03 June 2019
- UN DESA (2017) *International migrants stock*. <https://www.un.org/en/development/desa/population/migration/data/estimates2/estimatesgraphs.asp>. Accessed 03 June 2019



# Israel's Approach Towards Space Security and Sustainability

# 32

Deganit Paikowsky, Tal Azoulay, and Isaac Ben Israel

## Contents

Introduction .....	590
An Overview of Israel's Space Activities .....	591
Israel's Perspectives on Space Security and Sustainability .....	596
Conclusion .....	598
References .....	598

## Abstract

In the last 30 years, Israel developed an indigenous space capability to launch, develop, operate, and maintain satellites in two main niche areas: Earth observation and communications, including the ground segment of communications satellites. Israel's space program was born out of national security needs. However, it has led to the growth of a commercial space sector. Recent years have seen Israel expand its cooperation with international partners as well as establish a civilian space policy backed with modest government funding. Space-related academia has begun partnering more with government and businesses, and space start-ups have sprouted, a notable though noncommercial example being SpaceIL. What began as a purpose-focused defense necessity has blossomed into a diversified amalgam of enterprises, academia, and government dealing in a broad spectrum of space endeavors. Space activities are seen as contributing significant and cross-cutting benefits to Israeli society from early

The views expressed are solely the authors' and do not reflect an official policy or opinion of any Israeli entity.

D. Paikowsky (✉) · T. Azoulay · I. B. Israel  
Yuval Neeman Workshop for Science, Technology and Security, Tel Aviv University,  
Tel Aviv, Israel  
e-mail: [deganit.paik@gmail.com](mailto:deganit.paik@gmail.com); [tal.azoulay.ssp11@gmail.com](mailto:tal.azoulay.ssp11@gmail.com); [itzik@post.tau.ac.il](mailto:itzik@post.tau.ac.il)

education to an advanced economy and all points in between. Within the context of protecting and encouraging this nationally important ecosystem, Israel considers international space security, safety, and sustainability to be of importance. As such Israel actively promotes this position through its own space activities and increasingly in international forums.

---

## Introduction

Since its establishment, Israel has suffered from acute security threats beyond its immediate borders. Israel's needs to relate to a broad circle of states which surround it demand an orientation towards space. As a result, Israel's space program was developed to fulfill acute national security needs. This mainly involves early warning, intelligence, deterrence, and self-reliance in advanced technologies. As a small country, which suffers from limited resources, the country adopted a pragmatic approach to space.

Israel's pragmatic approach contends that Israel's space program includes the capability to build, operate, and launch remote sensing satellites into space, as well as develop and operate communication satellites. Israel does not undertake to build all systems entirely on its own. It has, for example, no navigation or weather satellites, and has no indigenous human spaceflight missions. However, Israel increasingly cooperates with international partners on projects of this nature, as well as scientific projects.

It is important to note that the overall space activity of Israel is much broader than national security activity. Almost a decade ago, the Israeli government adopted an official civil space policy and began modestly funding civilian space activities. Israel also has a strong scientific sector as well as commercial space activity. In this regard, Israel has long-established space industries but also start-ups and innovative space initiatives, including educational initiatives. For example, numerous nano-satellites designed and built by high school students. Some have already been launched and successfully operated, while many others are in development.

Israel's long legacy as a spacefaring nation, and the development of its space ecosystem, demands an orientation towards space security and sustainability. Therefore, Israel attributes great importance to securing the space environment for peaceful uses for all nations. This interest extends beyond security needs; should outer space become inaccessible and unsafe, this will negatively impact Israel's overall space activities.

This chapter analyzes Israel's overall approach to space security and posits that Israel's approach to space security may be described as threefold: (1) promoting a robust and diversified space sector that provides for Israel's national security needs and protecting and safeguarding Israel's space assets, systems, and capabilities; (2) competing in the global space market and encouraging new space capabilities and activities; and (3) maintaining a safe and sustainable space environment for all users.



This chapter contains two primary sections. The first section provides a detailed overview of Israel's space activity. The second section provides an analysis of the Israeli perspective related to space security.

---

## **An Overview of Israel's Space Activities**

Israel first built its presence and strength in space in accordance with priorities that correspond to its national and security needs. Therefore, understanding Israel's perception of space and of space security demands an analysis of Israel's strategic conception in relation to space (Ben Israel and Paikowsky 2017).

Israel's security conception is based on the profound understanding that it suffers from a significant quantitative inferiority against its rivals. To overcome this numeric disadvantage, Israel's leadership has chosen to focus its efforts on the development of a qualitative edge. In this perspective, Israel's space program plays a significant role in the country's overall answer to its strategic challenges. First, Israel's space program provides significant tangible capabilities to deal with the threats imposed by Israel's enemies. Second, and equally important, a national space program, which includes the ability to develop and to launch satellites into space, indicates very advanced national capabilities. Israel's achievements in space, whether civilian or military, project a clear message of national might. They emphasize the qualitative gap between Israel and its neighbors; they contribute to the country's accumulated achievements, aimed at deterrence; and philosophically, they reinforce the image of the "Iron Wall" in the eyes of its enemies, i.e., a power which cannot be overcome easily. All of that is accomplished without articulating an explicit military threat, which could provoke an unwanted and dangerous chain reaction in the region (Ben Israel and Paikowsky 2017).

More specific and tangible is the role the space program fulfills in mitigating the challenge of Israel's lack of strategic depth and acute need of early warning caused by Israel's narrow borders. Under these geopolitical circumstances, it was necessary to avoid the elements of strategic surprise and sudden attack. For these reasons, Israel's security doctrine demands advanced intelligence capabilities for early warning, as well as combat capabilities for a rapid transfer of battle away from Israel's population centers. The orientation towards space assists Israel in coping with the challenges presented by the lack of strategic depth and need to provide early warning.

With this in mind, the major impetus leading to the decision to embark on an independent Israeli space program was the 1979 Egypt-Israel Peace Treaty, and the perceived need to protect Israel, including through the need to verify Egypt's compliance with the treaty. The treaty did not neutralize Israel's concerns of hostile Egyptian aspirations. Moreover, Israel was to withdraw from the Sinai Peninsula. The greater distance from Egyptian territory meant that the Israeli military lost much of its early-warning intelligence-collection capabilities, including the ability to carry out manned reconnaissance flights over the Sinai Peninsula, now part of the

Egyptian sovereign state. (Such flights were considered a violation of Egyptian sovereignty and were a very sensitive issue in the embryonic relations between the two countries.) Therefore, there was a clear need for intelligence on what was happening in Egypt without violating its sovereignty. One of the potential solutions to the early-warning problems was using reconnaissance satellites. (For a review of the history of Israel's space effort, see: Paikowsky, D., "From the Shavit-2 to Ofeq-1-A History of the Israeli Space Effort", *Quest*, Vol. 18, No. 4, Fall 2011, pp. 4–12.) In 1981, the Israeli space program was established out of a pragmatic approach aimed to satisfy national security needs of early warning, deterrence, and self-reliance in advanced technologies. In 1988, Israel successfully launched its first satellite – Ofeq-1. "Ofeq" would become a very successful line of increasingly advanced earth observation capabilities.

The opportunity to observe Earth from space is a technological solution which enables Israel to cope with threats from hostile countries directly bordering the country, as well as those that threaten Israel but are located farther away geographically. At the 2013 Ilan Ramon Space Conference, the then Israeli Air Force Commander, Major General Amir Eshel, clearly stated the value of Israel's space capabilities as relates to strategic depth. "The threats we must deal with come from the border fence and from far away. Today, space is our strategic depth and it is what allows us to maintain our qualitative advantage. Thanks to our indigenous satellites, our ability to operate at any distance increases tremendously." (Chanel and Michael 2013).

The Israeli space program is recognized as a critical component of its independent intelligence capability. However, the issue of Israel's self-sufficiency is a complex one, and as a small country, Israel cannot be completely self-reliant. Nevertheless, in the field of intelligence, Israel has a great deal of autonomy.

Possession of independent intelligence capabilities has many implications for Israel beyond the field of intelligence. It enhances the power of the state and the image of Israel in the eyes of its opponents as well as its allies. It provides flexibility, both in its ability to collect information and the resulting autonomy in decision-making. Independent capabilities also permit the country to conceal its operational plans and areas of interest and to collect information unhindered. The space program is an important building block of this capability. To achieve this independence, Israel has continued to build its space program, especially the capability to develop and launch reconnaissance satellites.

Israel's space program also contributes to its deterrence. The following statement by Major General (Ret.) David Ivri, former Air Force Commander (1977–1982) and later Director General of the Ministry of Defense, provides valuable insight into the role of the Israeli space program in Israel's deterrence strategy:

The perception of one's capabilities and one's willingness to use those capabilities are important components of deterrence. The perception of space capabilities is one of the primary components in Israel's future deterrence. Therefore, Ofeq 1, 2, and 3 contributed far more than anyone estimated. Imaging resolution is not the strategic measurement. Rather, the strategic measurement is the perception of capabilities that the State of Israel displays.

Not what we possess, but rather what the enemy estimates that we possess. The gaps in capabilities and information, in the tactical field, miniaturization field, and others are an immeasurably important component in the dimension of our strategic deterrence. (Ivry 2006)

Despite the obvious attention that national defense reconnaissance satellites receive, the fact that Israel was able to attain independent launch capacity is justifiably considered a significant achievement. Israel remains one of very few countries in the world with this capability. This is despite the fact that Israel is the only country which launches its' rockets to the west, against the rotation of the earth, to avoid launching eastward over neighbors with which it has strained relations. Launching to the west incurs a "cost" of approximately one-third of boost efficiency which leads to significant constraints on payload weight. Israel overcame this disadvantage by developing expertise in miniaturization of components. This expertise is one of many which eventually were able to serve the development of commercial space presence.

In the 1990s, Israel's space industry followed in the footsteps of many other technological sectors that were originally related to defense and began commercial spin-offs. As such, Israel developed commercial platforms such the Amos communication satellite series, EROS remote-sensing electro optical series, sub-systems, and other equipment.

In the last decade, the national space activity of Israel underwent a comprehensive process of re-evaluating its goals, objectives, and policies. In November 2009, a national task force was appointed to reexamine the Israeli space program and recommend a new framework. (The task force was headed by Mr. Menachem Greenblum, Director General Ministry of Science and Technology and Prof. Isaac Ben Israel, Chairman of the Israeli Space Agency.) The main objective of the task force was to focus on civilian applications and scientific activity that would allow Israel greater industrial scale and competitiveness in the growing world space market. The task force submitted its report and recommendations in June 2010 (Paikowsky and Levi 2010). The report outlines Israel's strengths, weaknesses, opportunities, and challenges for achieving its goals in space. Scrutinizing all of these parameters, the task force argued that Israel has great potential to lead in space technology in specific areas, but because of insufficient investments, Israel is in danger of gradually losing its competitive edge. In order to upgrade the scale of the local space industry, it was suggested that the Israeli government prioritize a national civilian space program focused on developing and renewing infrastructures, supporting academic research, and promoting international collaborations with other spacefaring nations, as well as with developing nations. In 2011, the Israeli Parliament established a subcommittee dedicated to space matters. In December 2012, after careful review by the treasury officials, the Finance Ministry approved an investment of \$50 million for Israel's new civil space program (The Marker 2012).

On the basis of this new funding, the space agency began implementing a new space program, geared towards R&D and modernization of its civilian space activities. Among the program's objectives are advancing the local space industry, strengthening academic research, and raising the Israeli public's awareness of

space activities and research, as well as reinforcing and expanding international cooperation. For example, in 2017, Israel and France launched Venus, a jointly developed and run environmental satellite. Following the success of Venus, the Israeli and French space agencies signed a statement of intent in 2018 to develop a new environmental project called C3IEL, which will involve a constellation of three nano-satellites focusing on climate research (CNES 2018). Among its efforts in these directions is also hosting of prestigious international conferences. In 2015, Israel hosted the annual International Aeronautical Congress and in 2016 hosted the Space Studies Program of the International Space University.

In September 2016, the communication satellite Amos-6 was lost on SpaceX launch-pad. Consequently, the Ministry of Science and Technology initiated a national task force to review the state of Israel's communication satellites. The report was submitted in December 2016 pointing to the need for a comprehensive and long-term program to upgrade capabilities to develop the new generation of Israeli made communication satellites. (For a detailed overview of Israel's Communication satellites, as well as the report of the 2016 Task-force, please see National Report by the state comptroller number 69A published in October 2018. Available at: [https://www.mevaker.gov.il/he/Reports/Report\\_642/5caecf12-5145-4007-a355-83731735b0c1/2018-69a-304-Lavyanim.pdf](https://www.mevaker.gov.il/he/Reports/Report_642/5caecf12-5145-4007-a355-83731735b0c1/2018-69a-304-Lavyanim.pdf). Accessed on April 14, 2019.) Two years later, in September 2018, Israel's government approved the development of Amos-8. The development of future satellites is yet to be decided. (For additional information about the decision, see: <https://www.space.gov.il/news-space/131329>. <https://www.space.gov.il/news-space/131329>. Accessed April 14, 2019.)

Israel is often referred to as the Start-Up Nation, and this is true as well for the space field. Following the impressive defense-related space advances and subsequent commercial space enterprises, a vibrant community of space start-ups has sprung up in Israel. The activities of a number of start-up companies, like SpacePharma and Effective Space Solutions, are noteworthy. (For additional information about these companies, see: <http://www.effective-space.com> and <http://www.space4p.com/>) Effective Space Solutions, in particular, is proposing solutions that are directly linked to increasing the safe extension of lifespan for satellites.

Aside from these initiatives, various educational projects have evolved as well, such as the Herzliya Science Center Space Lab, which is located in a high school. In 2014, this project launched its first nano-satellite, Duchifat-1, which was built by high school students (Winer 2017). Duchifat-2 was launched 3 years later in 2017. A year later in 2018, the Israel Space Agency initiated a new project dedicated for high schools in which seven high schools around the country will be able to plan and build their own innovative nano-satellites. The project will enable students to participate in the design and construction of these satellites. All seven satellites will be launched at the end of the process as one constellation that will serve as a communications network for transmitting information from space. (More information is available on the Israel Space Agency website: <https://www.space.gov.il/news-space/131327>. Accessed on April 15, 2019.) Recently, this initiative evolved into an even larger project and to an establishment of a dedicated research center for small satellites at Tel Aviv University.

Another particularly profound educational initiative is SpaceIL. This project began as a competitor in the GoogleX Prize to land a spacecraft on the moon. Despite the later cancellation of the GoogleX Prize, SpaceIL continued and in February 2019 launched its spacecraft aboard a SpaceX Falcon-9 launcher. Several weeks later, it succeeded putting its spacecraft “Beresheet” into lunar orbit, making Israel only the seventh country to achieve this feat. Unfortunately, the landing was not successful and the craft crash-landed on the lunar surface on April 11, 2019. Not to be deterred, SpaceIL has already begun working on a follow-up mission. In addition to the mission goal of landing on the moon, the SpaceIL team sees their mission also as educational and cultural. SpaceIL team and volunteers consistently lecture at schools and other public events to encourage youth involvement in STEM subjects in order to advance “a Beresheet Effect” in the Israeli society. It is important to note that SpaceIL is a private-commercial initiative and not governmental. (According to GoogleX Prize, governmental funding had to be very limited.)

There are also a number of more “formal” educational initiatives aiming to provide special space-oriented programs to schools around Israel from elementary school up through high school. The Ministry of Science and the Israeli Space Agency collaborates with the Ministry of Education to encourage interest in STEM subjects based on the understanding that space serves to inspire youth (and young professionals).

The increasing place of commercial and civil space activities is also noticeable in recent conferences and forums taken place in Israel. The Ilan Ramon International Space Conference has developed into an important date on the international space community’s calendar, consistently attracting the attendance of many heads of space agencies, industry leaders, and decision-makers. Its most recent annual meeting (14th meeting), which took place in January 2019, focused on commercial space (Ramon14.forms-wizard.net 2019). In addition, for the first time, the conference was preceded by a special workshop dedicated to space entrepreneurship.

On top of that, the Ramon Foundation, which is a nonprofit organization set up in memory of Israel’s first astronaut Ilan Ramon and his son Asaf Ramon, has set as one of its main objectives “to help engineers and entrepreneurs in their first steps in the space industry.” To this end, the Foundation assists in networking, knowledge sharing, hackathons, and conferences (Ramon Foundation 2019).

To conclude this part, the rationale for Israel’s engagement in space activities described above reveals that Israel, which operates a successful space program on a modest budget, views space as a significant opportunity, especially as a force multiplier projecting the quality of force over its quantity in the most broadly manner. Retired Brig. General Amnon Harari, Head of Space Programs in the Israeli Ministry of Defense, stated clearly “Beyond the defense needs for which our satellites provide solutions, the Israeli space industry represents an important component [for Israel] in terms of the economy, education, advancing technology, science, small businesses, start-ups and more.” (Shoval 2018).

This opportunity is accompanied by significant challenges, especially in maintaining its’ qualitative advantage and preserving Israel’s position at the forefront

of technology. The significance of space in Israel's strategic conception and its long term and growing space capabilities in the defense, civilian, and commercial fields leads Israel to look for ways to protect its satellites, as well as shape its perspective on space security. The next section provides an overview and an analysis of Israel's perspectives and activities regarding space security and sustainability.

## **Israel's Perspectives on Space Security and Sustainability**

Israel attributes great importance to space security and sustainability. This interest extends beyond security needs and derives also from the interest to compete in the global space market and encouraging new space capabilities and activities, as well as maintaining a safe and sustainable space environment for all users. Should outer space become inaccessible and unsafe, this will negatively impact Israel's overall space activities.

At the heart of Israel's approach to advancing space security and sustainability is promoting a robust and diversified space sector that provides for Israel's national security needs and protecting and safeguarding Israel's space assets, systems, and capabilities. For example, the following statement was made by Commander of the Israeli Air Force, Eliezer Shkedy, at the 2007 Ilan Ramon Annual Space Conference: "the operational importance of space is increasing constantly. Why is this field critical? There exists a concern that others who recognize its importance will try to attack space assets. We must consider defense measures, against physical harm, jamming, blinding, or any other technique. One of the greatest surprises that can happen in the modern world, in advanced countries with space assets, is a situation in which a country is surprised to find its space assets damaged." (Shkedy 2007). Shkedy's statement is an example of the growing recognition in Israel of the importance of the need to protect space systems. In this regard, one direction recognized by many in Israel is the likelihood of soft interference in space systems, especially the ground segment, through cyberattacks and therefore the need to protect space systems against this threat. (For more information on Israel's cyber policies, see: Tabansky and Ben Israel (2015).)

Another effort on this regard is in the field of Space Situational Awareness (SSA). SSA is one of the fields in which Israel looks for international cooperation. In 2015, Israel signed a data-sharing agreement with the US STRATCOM for Space Situational Awareness. This agreement enables Israel to benefit from the collective data of dozens of countries and many commercial entities to avoid collisions with satellites and space debris (Pomerleau 2019).

Due to this kind of collaborations, Israel's perspective on space security and sustainability is broad and includes concern for the continued smooth operation of those other parties' capacities as well as cooperation and collaboration with some of those partners. Therefore, maintaining a safe and sustainable space environment for all users is also an important objective of Israel's perspective regarding space security. In order to achieve this goal of greater space security and sustainability for all users, Israel is actively looking to contribute to a sustainable space

environment. In this capacity, Israel shares the idea that achieving the goal of space security and sustainability requires international collaboration and development of best practices for responsible behavior. In this regard, Israel recognizes the significance of contributing to multinational efforts. Joining the US efforts to improve Space Situational Awareness for debris tracking serves as an example of Israel's general perspective that international efforts by responsible players will have positive effect on the sustainability of outer space (Azoulay 2019). By taking this step, Israel not only improves the protection of its own satellites but demonstrates that it sees itself as a party to the international effort of sustaining the space environment for global stability and security.

Another example to Israel's efforts to promote responsible, peaceful, and safe use of space is its greater involvement in UN-COPUOS. In 2015, Israel was voted in as a regular member of the UN Committee on the Peaceful Uses of Outer Space [COPUOS] (United Nations 2015). By 2017, Israel was voted to serve on the six-member Steering Bureau of COPUOS (Israeli Ministry of Foreign Affairs 2017). These developments speak not only to Israel's decision to increase its international cooperation but also the positive feedback and support Israel is receiving from the international space community. In this capacity, Israel is contributing to diverse activities of COPUOS. One such activity is Planetary Defense. "Israel Space Agency is making efforts to find unique ways to contribute to planetary defense efforts. Specifically, Israeli researchers are conducting studies in order to contribute the world's effort." (Statement to UN-COPUOS by Israel's Space Agency delegate at the STSC 2019.)

Last but not least, due to the understanding in Israel of the need for international cooperation to ensure that space remains accessible and sustainable for the future, Israel favorably views legally nonbinding efforts towards space sustainability. For example, The European Union proposed an Outer Space Code of Conduct. (For the updated version of the European initiative of the Outer Space Code of Conduct dated June 2012, please see: [http://www.consilium.europa.eu/media/1696642/12\\_06\\_05\\_coc\\_space\\_eu\\_revised\\_draft\\_working\\_document.pdf](http://www.consilium.europa.eu/media/1696642/12_06_05_coc_space_eu_revised_draft_working_document.pdf).) In 2012, an interministerial team of space experts was put together to discuss the code and its implications for Israel. An Israeli delegation actively participated in the open-ended consultation, which took place in Luxembourg in May 2014, as well as at the negotiations which took place in New York in July 2015.

Israel was also favorable towards more recent efforts to advance space as a secure and sustainable environment taken by UN-COPUOS. The following Israeli statement reflects on its overall approach: "Israel perceives space as a global commons and therefore aspires to contribute to a secure and sustainable space environment. Our small country acknowledges the worldwide use of space for supporting sustainable activity for development, as well as to promote contribution to UN system and its Sustainable Development Goals. Israel, through the Israel Space Agency, seeks greater international collaboration and cooperation, especially among democratic spacefaring nations, in maintaining space as a peaceful environment for the benefit of all." (UN-COPUOS 2018 General exchange of views, Israel delegation.)

## Conclusion

In conclusion, Israel's space program was launched in response to national security needs. Over the years, with Israel's development and evolution as a country, its needs and capabilities have also evolved. Today, Israel has commercial, scientific, and civilian space assets and is expanding its involvement in international space cooperation. These developments, combined with increasing reliance on space for day-to-day activities and the nation's continuing security issues, make space security a concern for Israel and demand orientation to space sustainability on a diverse range of perspectives and activities. For example, as the local civil and commercial space activity of Israel grows and flourishes, there will be a greater need to update national regulations regarding space security and sustainability. On the international level, as these global trends of advancing space technologies and reliance on space systems and capabilities continue to grow, the need of maintaining the space environment safe and secured will only rise. Hence, Israel will continue to support global efforts to promote responsible behavior and pursue partnerships of this kind.

## References

- Azoulay Y (2019) Yisrael v'Arhab Yishatfu Peula Kdai L'mnoa Hitnagshuyot Bein Lavyanim c'Halal ]Israel and USA will cooperate to prevent crashes between satellites]. [online] Globes. <http://www.globes.co.il/news/article.aspx?did=1001061882>. Accessed 4 Feb 2019
- Ben Israel I, Paikowsky D (2017) The iron wall logic of Israel's space programme. *Survival* 59(4):151–166
- Chanel L, Michael T (2013) Ha Halal Hu Ha'Omek Ha'astrategi [Space as strategic depth]. [online] Israeli Air Force. <http://www.iaf.org.il/4391-40401-he/IAF.aspx>. Accessed 12 Jan 2019
- CNES (2018) France-Israel Space Cooperation. <https://presse.cnes.fr/en/france-israel-space-cooperation-cnes-14th-ilan-ramon-conference-news-space-venms-and-c3iel-focus>. Accessed 15 Feb 2019
- Israeli Ministry of Foreign Affairs (2017) Israel elected to UN Space Committee. [online] <https://mfa.gov.il/MFA/PressRoom/Pages/Israel-to-Lead-.aspx>. Accessed 18 Apr 2019
- Ivry D (2006) Hahalal Kezira Estrategit Ba'avar, Bahove, Veba'atid [Space as a strategic arena in the past, present and future]. Fisher Institute for Air and Space Strategic Studies, Hertzliya, Israel, p 50
- Paikowsky D, Levi R (2010) Space as a national project – an Israeli space program for a sustainable Israeli space industry, presidential task-force for space activity final report. Israel Ministry of Science and Technology, Jerusalem
- Pomerleau M (2019) Stratcom expands space surveillance with Israel agreement – Defense Systems. [online] Defense Systems. <https://defenseystems.com/articles/2015/08/13/us-stratcom-israel-space-surveillance-agreement.aspx>. Accessed 9 Jan 2019
- Ramon Foundation (2019) Ramon Foundation. [online] <http://ramonfoundation.org.il/>. Accessed 9 Jan 2019
- Ramon14.forms-wizard.net (2019) 2019 conference agenda. [online] <https://ramon14.forms-wizard.net/website/index>. Accessed 20 Feb 2019
- Shkedy E (2007) Address at the 2007 Ilan Ramon annual space conference, Fisher-Institute for Strategic Air and Space Studies, Herzliya
- Shoval L (2018) Images revealed of Israel's first satellite launch. [online] Israelhayom.co.il. <https://www.israelhayom.co.il/article/587527>. Accessed 24 Jan 2019
- Tabansky L, Ben Israel I (2015) Cybersecurity in Israel. Springer,



- The Marker (2012) State will invest 90 million shekels in international space cooperation. <https://www.themarker.com/news/macro/1.1826164>. Accessed 2 Mar 2019
- United Nations (2015) Fourth Committee approves four draft texts, concludes general debate on questions relating to information | Meetings Coverage and Press Releases. [online] <http://www.un.org/press/en/2015/gaspd593.doc.htm>. Accessed 2 Feb 2019
- Winer S (2017) Nanosatellite built by Israeli high-schoolers blasts into space. [online] Timesofisrael.com. <https://www.timesofisrael.com/nanosatellite-built-by-israeli-high-schoolers-blasts-into-space/>. Accessed 1 Apr 2019



# Policies and Programs of Iran's Space Activities

# 33

Hamid Kazemi and Mahshid TalebianKiakalayah

## Contents

Introduction .....	602
International Space Policy .....	604
National Space Policy .....	604
Vision Plan .....	604
The Comprehensive Scientific Map of Iran .....	606
The Comprehensive Document of Aerospace Development .....	607
The Five-Year Iranian Economic, Social and Cultural Development Plans .....	610
Supervisory and Regulatory Structure for Implementing Space High-Level Policy Documents .....	612
Challenges on Implementing High-Level Iranian Space Policy Plans and Documents ...	614
A Glance at the Space Security of Iran .....	615
Conclusion .....	617
References .....	618

## Abstract

Iran pursues its space activities, through international and national space policies, in accordance with international space treaties and ensuring the peacefulness of its space activities. At international level, Iran has prioritized international cooperation and compliance with international space regulations. It has always taken steps toward the peaceful use of space by playing an effective role in the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS), signing international space law treaties, membership in international and regional space organizations, and cooperation in the implementation of joint international space

H. Kazemi (✉)

Research Institute, Department of Air and Space Law, Tehran, Iran  
e-mail: [h.kazemi@ari.ac.ir](mailto:h.kazemi@ari.ac.ir)

M. TalebianKiakalayah

Graduate of Islamic Azad University, Tehran North Branch, Tehran, Iran  
e-mail: [mahshid.talebian@yahoo.com](mailto:mahshid.talebian@yahoo.com)

projects. Its national space policy which was triggered by the commencement of its national space activities has been defined accordingly. In addition, principles for the regulation of space activities have been codified and implemented based on high-level national documents including the Vision Plan, the Comprehensive Scientific Map of the Country, the Five-Year Development Plan Rules (Fourth to Sixth), and the Comprehensive Document of Aerospace Development. These documents outline the scope of space activities and technologies while securing space security and ensuring the peaceful uses of outer space. The responsible authorities for space are proceeding to develop space technologies and activities based on the provisions in these documents. According to the policy, Iran ultimately aims for technology development and satellite operation as well as sounding rockets that provide civil services and also ensure the presence of Iranian astronauts in outer space. These goals are based on the principle of international cooperation and peaceful uses and exploration of outer space.

---

## Introduction

Since the development of the space industry, space security has been a core matter of attention for the international community, maintaining throughout the years a prominent role in space activities and the economic growth of countries (Bockel 2018). In recent years, the development of space science, space technologies, and space applications for civilian purposes have had significant effects on people's daily lives (Concini and Toth 2019). In this context, the Islamic Republic of Iran (Iran) has put a particular focus on the space industry and on the use and exploration of outer space for national scientific, economic, social, and cultural development. Consequently, Iran has focused its national policies on this issue.

Iran has taken the potential of space into consideration as reflected in the Iranian national and international policy making. The competent space authorities have actively specified the space strategy and goals that contribute to the development of space technology and space activities. At international level, the space authorities promote the peaceful exploration and use of outer space in pursuit of ratifying and applying international space provisions. In parallel they attend international fora and in particular the UN Committee on the Peaceful Uses of Outer Space (UNCOPUOS). At national level, the space strategy concerning Iran's space activities has been codified in its high-level national documents. Iran's international strategic space policy, developed in discussions taking place at international fora such as the United Nations, has placed particular emphasis on the peacefulness of space activities. The involvement of Iran since the dawn of the space age in the international community – by becoming the 24th member of the UNCOPUOS in 1961 – can be attributed to its early motivation and aspiration to participate in the space sector (UNCOPUOS membership).

Iran has brought two main aspects of space activities into focus of its national strategic space policies. First, it takes the development of space activities into consideration so as to ensure national security and sovereignty of Iran over its

territory. Second, by developing such activities, it intends to provide better services to the citizens through the use of space applications. Namely, surveillance and communication satellites are able to provide appropriate services in sectors such as agriculture, telecommunications, and transportation (Blount 2010). The allocation of dedicated budgets to authorized space organizations, as set out in Iran's high-level national documents, indicates the importance of space for the strategic position of Iran. Long-term plans for the space sector have been outlined in high-level legal documents that outline the implementation of development programs. Relevant documents include the 20-Year Perspective Document, the Comprehensive Scientific Map of the Country, the Five-Year Development Plan Rules (Fourth to Sixth), and the Comprehensive Document of Aerospace Development, which will be discussed in the next section (Islamic Republic of Iran 2013).

Since the late 1990s, with the aim to develop peaceful space activities, Iran has actively pursued the development of satellite communications and sounding rockets (Global Security 2010). To achieve international cooperation in space, Iran began cooperating with Russia in the 1990s regarding the development of civilian satellites for communication and imagery, followed by cooperation with China and Thailand in 2008 concerning the launch of a satellite for surveillance and response to natural disasters. In addition, Iran has cooperated with other countries in the region, particularly allied countries, as well as European countries. In 2003, Iran, as the first Islamic country in the region aiming to develop space activities, decided to launch a satellite into orbit. Iran operated its first satellite, Sina-1, which launched with a Russian satellite launch vehicle from Russia. Since then, Iran has declared itself as the 43rd country with its own satellite capacity, which was a landmark in the history of Iranian space activities.

Iran has stated that the satellite is used for imagery of Iran, in particular for controlling and monitoring natural disasters. During this period, another satellite, Omid, was presented as the first made Iranian satellite. On February 2, 2009, this satellite was launched by Safir Satellite Launch Vehicle (SLV), a domestic launch vehicle (Tarikhi 2009). This was a big step forward for Iran that it enabled it to enter the league of space-faring nations. Omid was equipped with experimental satellite control devices and power supply systems. It was also designed for gathering information and testing equipment. Iran's space program up to that point had been based on ground stations that relayed Intelsat communications and received Landsat data (Tarikhi 2009).

With regard to Sounding Rocket Vehicles (SRV), in February 2007, Iran tested an SRV for research purposes which was followed by SRV 1. SRV 2, which was successfully launched into space, provided the opportunity for Safir SLV to launch the first national satellite, Omid. Iran's space program up to that point had been based on ground stations that relayed Intelsat communications and received Landsat data (Tarikhi 2015). The success of this launch placed Iran alongside the eight countries with the ability to put their own space-built objects in orbit. It has been explicitly stated that this satellite is used for peaceful purposes and in particular for agricultural and economic purposes. The launch of SRV 3 took place in 2010, demonstrating a new capacity in space technology development for Iran (Harvey et al. 2010). As a

result, Iran has made its space activities debut as one of new space farers with access to space through of the development and launch of satellites and SRVs directly and indirectly. The access of Iran to space has been recognized as a necessity for the protection of national interests. This research seeks to investigate the goals, strategies, and long-term space policies that have been outlined in Iran's high-level national documents.

---

## International Space Policy

Taking into consideration the central role of UNCOPUOS in space, Iran has been involved in deliberations for the formulation of international space treaties in the 1960s and the resolutions that followed. Iran has signed the Outer Space Treaty 1967 and the Registration Convention 1975 and has also ratified the Liability Convention 1972 and the Rescue Agreement 1968. Iran has not signed the Moon Treaty 1979 ([UN Treaties](#)). As a regional influential country, Iran has always placed importance on peaceful space activities. The 1970s was the dawn of Iran's space activities. The most important initial steps marked the establishment of the Remote Sensing Organization, the registration of orbital slots in 1974, the membership to the International Telecommunication Union in 1967, and the membership to UNCOPUOS in 1969 ([UN Treaties](#)). The current status of Iran's participation in international space treaties and its membership in international and regional organizations related to space activities are shown in Tables 1 and 2.

---

## National Space Policy

The body of general policies of the regime is a new foundation which was contained in the Constitutional Law (Islamic Republic of Iran 1989) after the Islamic revolution of Iran in 1989. Determining the national policies falls under the responsibility of the Supreme Leader. After consultation with the Expediency Discernment Council, their implementation is announced. The general policies are determined based on national principles and goals that lay down the guiding framework for the orientation of the country in all governmental areas, including space activities. This system allows for a reasonable approach toward the accomplishment of its goals. Long-term space policies and programs are developed in three high-level national documents including the Vision Plan, the Map, and the Document of Aerospace Development, as well as the Five-Year Development Plans that are approved and implemented by the Cabinet.

## Vision Plan

The 20-Year Vision Plan of Iran (Islamic Republic of Iran 2003) is a document determining Iran's development in numerous aspects consisting of cultural, scientific, economic, political, and social fields which are codified by Expediency

**Table 1** Status of Iran's participation in international treaties of outer space

United Nations International Space Treaties	Action	Name of treaties/conventions	Date of notification/ deposit
	Signature	Outer Space Treaty	1967
	Signature and ratification	Rescue Agreement	1968
	Signature and ratification	Liability Convention	1972
	Signature	Registration Convention	1975
	–	Moon Treaty	1979
Related agreements	Signature and ratification	Treaty banning nuclear weapon tests in the atmosphere, in outer space, and under water (NTB)	1963
	–	Convention relating to the distribution of program-carrying signals transmitted by satellite (BRS)	1974
Cooperation organizations' conventions	Signature and ratification	International telecommunications satellite organization (ITSO)	1971
	–	International system and Organization of Space Communications (Intersputnik)	1971
	–	European Space Agency (ESA)	1975
	–	Agreement of the Arab Corporation for Space Communications (ARB)	1971
	–	Agreement on cooperation in the exploration and use of outer space for peaceful purposes (INTC)	1971
	Signature and ratification	International Mobile satellite organization (IMSO)	1971
	–	European telecommunications satellite organization (EUTELSAT)	1982
	–	European Organization for the Exploitation of meteorological satellites (EUMETSAT)	1983
	Signature and ratification	International telecommunication constitution and convention (ITU)	1992

Discernment Council of the country (Islamic Republic of Iran 2013, Article 9). In implementing the Plan from 2005 to 2025, Iran aims to obtain the first economic, scientific, and technological position in the South West Asian region and to be recognized as a developed country equipped with advanced knowledge, security, independence, power, and autonomy. The Plan is the basis of Five-Year Development Plans and regulations which outline the overall direction of activities in different aspects. It falls under the Constitutional Law and regulates the framework within which the general polices are regulated. It should be considered as a source of

**Table 2** Status of Iran's membership in other international governmental and intergovernmental organizations

Membership of Iran	Headquarter location	Authorized organization	Number of states parties	Name of organization	Established
	Vienna-Austria	Ministry of Foreign Affairs and Iranian Space Agency	86	COPUOS	1959
	Geneva-Switzerland	Ministry of Information and Communications Technology of Iran	143/193	ITU	1865
	Beijing-China	Iranian Space Agency	9	APSCO	2005
	France-Paris	Aerospace Research Institute	66 out of 300	IAF	1951

the state's comprehensive policy through which the approach of Iran's space activities should be organized in developing a strategic industry.

According to the Plan, Iran shall take steps to increase its role in the world's scientific outputs aiming at organizing and mobilizing the country's capabilities and facilities. The aim is to strengthen the software movement and promote research capacity as well as acquisition of technology, especially new technologies including sub-technologies, biotechnologies, information and communication, environment, and aerospace. As it can be witnessed, the Plan, which is the most important document for the future policy making of the country, has addressed Iran's contribution to producing science in the world and acquiring new technologies, particularly aerospace technology.

There is no reservation that active presence in outer space is one of the great achievements that has been predicted in the Vision Plan. The objectives of the Plan are met with sufficient investment, the efforts of national experts, and cooperation with other countries. Furthermore, the Plan outlines the prospect of reinforcing national authority and security with an emphasis on scientific and technological growth. In other words, this Plan recommends taking steps to enhance security and promote the global position in parallel to the development of science and technology, such as the aerospace sector. Regarding the implementation of the plan in the aerospace sector, a number of additional fundamental high-level documents have been developed, including the Comprehensive Scientific Map of the Country, the comprehensive aerospace development document and development plans.

## The Comprehensive Scientific Map of Iran

Living in the age of knowledge, countries need a plan to promote science exploitation; otherwise they will not be able to enhance or maintain their position. The Plan has revealed the general frontiers of Iran movement toward the future. In order to

achieve the goals, policy makers decided to chart Iran's scientific roadmap: a Comprehensive Scientific Map of the Country which clarifies the paths to access these goals. In other words, the required paths to achieve the outlined goals in the plan are determined by this Map, which was approved for science and technology areas. The Map was ratified by the Supreme Cultural Council of the Islamic Republic of Iran in 2011 (Islamic Republic of Iran 2011a). It is described as "a coordinated and dynamic set of goals, policies, and structures, planning requirements for strategic transformation of science, technology and innovation based on Iranian Islamic values to achieve the goals of the Plan." All executive organizations including state entities and private entities shall comply with its provisions. The main orientations or outputs of the Map should be implemented over the next two decades. The Map priorities focus on cognitive sciences, aerospace, and oil and gas, for which each of these specific documents has been prepared and approved (Islamic Republic of Iran 2011a).

The Map addresses two main issues including sending humans into space (human spaceflight) and designing, manufacturing, and operating satellites. According to that (Islamic Republic of Iran 2011a, No 9, Para 2–2), achieving these goals is mirrored in international cooperation and the Islamic world cooperation with other countries as the subset of national long-term technological and scientific targets. In addition to that, aerospace technology is prioritized as an A level among three levels of A, B, C (Islamic Republic of Iran 2011a, Paragraph 2–3: technological and scientific priorities of a country). It is noteworthy that the amount of allocated resources and consideration of competent authorities are the center of this prioritization. Implementation of main priorities usually requires the attention and support of superior competent authorities and executives. Aerospace technology and space activities are one of the top and main priorities under support of superior competent authorities. The supervision of the implementation of the provisions and principles of the Map is carried out by a Strategic Committee. Its mission is to take care of executing the Map in a timely manner. The Committee is responsible for monitoring the proper implementation of air and space policies, which are provided in the Comprehensive Document of Aerospace Development, which will be reviewed as follows:

### **The Comprehensive Document of Aerospace Development**

The Comprehensive Document of Aerospace Development was adopted in 2012 in accordance with the Map. It seeks to implement the fifth chapter of the Map. Since Iran has a special status, the document emphasizes the characteristic capacities and capabilities of Iran for space activities such as capabilities in manufacturing, operating, and deploying satellites and spacecraft in outer space and exploitation of outer space and training aerospace experts in universities and research institutes based on a global large scale. The details of the Document, consisting of the development of aerospace-based science, technology, and knowledge-based industries of aerospace sector in Iran, familiarize us with the approach adopted by the legislators and policy makers. The Document not only governs all institutions and sectors, including



military and nonmilitary (governmental and nongovernmental), but also has the ability to define the exploration of air and space applications. The latter include media, telecommunications activities, imaging, remote sensing, and cargo transportation in air and space. The Document also concludes activities in the areas of education, research, acquisition and development of technology, industrial activities, and service provision (Islamic Republic of Iran 2013).

Due to the high speed of technological developments and the limited time to put these developments into practice, one of the most important features of the space industry would be the knowledge base feature. Since a large part of space activities is knowledge-based, the economic importance of the space industry in the region for the coming years has been amplified due to its estimated million-dollar labor market. The Document covers all ground-based and space-based services and products related to the use or exploration of outer space, including telecommunications, earth observation, remote sensing, navigation, space security, bio space, and space science. The scope of aerospace and defense sector has been defined to include all required operations and services in the aerospace sector that protect and defend the security of Iran promoting its military authority. In principle, it deals with strategies, fundamental values, and long-term aerospace policies that are common to the both the air and space sectors. The goals and strategies of each of them will be stated in order to examine common principles particularly in the space sector (Islamic Republic of Iran 2013).

### **Common Principles in Air and Space Activities**

The Document in this part deals with strategy part, fundamental values, and long-term aerospace policies.

#### **Air and Space Strategy**

Promoting national security and authority, surpassing in technological and scientific advancements in other fields, and benefits resulted from the spreading developed or localized technologies flowing to other sectors are the factors that will globally convert an Iran's aerospace sector to the strategic one. In this regard, recent achievements, particularly in designing, manufacturing, and operating satellites and other aircrafts, have increased national dignity and self-esteem which could ultimately pick the rank of Iran in front of international observers (Islamic Republic of Iran 2013).

The Document declares that space policy making should be pursued in a way through which Iran can achieve the following capabilities:

- Has an effective authority in national security.
- Be efficient and reliable in fulfilling the strategic and current needs of world and Iranian society.
- Compatibility with culture and Islamic values of Iranian.
- Ability to creating budgets for designing, developing, manufacturing products, and providing aerospace services.

- Being inspired in expanding the frontiers of knowledge and developing aerospace technology.
- Playing a pioneer role in other areas of science, technology, industry, and services.
- Knowledge based and capable to apply the recent scientific, research, and technological achievements (Islamic Republic of Iran 2013).

### **Fundamental Values**

The Document, like the map, emphasizes Iran's space activities when it expresses the of the national aerospace sector. The most important of these values can be centralized justice in the development of aerospace sector and the benefits of its achievements; fostering talent, creativity, innovation, risk-taking, and courage, paying attention to the principle of rationality in the long-term management of space domain; coordinating science and technology with the environment; promoting international cooperation, raising the spirit of cooperation, partnership, the responsibility of academics and related institutions; and recognizing all space resources including celestial bodies, orbits, and their exploitation under the justified legal system as a common heritage of mankind (Islamic Republic of Iran 2013).

### **Long-Term Aerospace Policies**

The Document outlines long-term Iranian aerospace policies. The most crucial of these policies are as follows:

Emphasis on production of indigenous science and development of related sciences, utilization of maximized internal capacity, enabling capacities; taking responsibility for maintaining and improving the environment; creating the maximum cooperation of private sector and addressing them with an emphasize on a role of government in policy making and supervision, observing diplomacy frameworks of national technology in international aerospace partnerships and activities; exploiting the surplus age of aerospace technology in other industrial and manufacturing sectors; observing passive defense and protecting of this technology to develop aerospace sector, absorbing elites as a major factor in technological developments; and last but not least creating the basis for economic and social activities in this sector maintaining sustainable security of Iran (Islamic Republic of Iran 2013).

### **Particular Principles in Space Activities**

The Document has specifically targeted goals to achieve the abovementioned purposes. These orientations can be categorized as follows:

- Reaching first place in the region in conquering space and dominance in space through relevant science and technology based on capabilities of national universities and research centers.
- Research and development of manned space missions.

- Designing, manufacturing, and operating national satellites in orbit with various applications such as communications and remote sensing with a priority on international cooperation.
- Access to space-based communications infrastructure to meet national regional, universal, public, and commercial requirements compatible with ground-based telecommunications platform.
- Achieving required technologies for remote sensing and ground observation with accuracy below 10 m.
- Cooperation in positioning, navigation, and timing on national and regional level in accordance with global and competitive quality.
- Designing, manufacturing, and operating satellites and carriage systems of defense and security satellites which are needed to insure national space security.
- Maximum usage of all state institutions and private sector to develop and promote space activities for long-term space programs of the country.
- Supporting privatization and providing necessary framework for space knowledge-based industries and companies.
- Supporting space educational and research activities.
- Development of international collaborations and interactions to carry out space programs.
- Applying space achievements to understanding the universe and developing astronomy (Islamic Republic of Iran 2013).

It further refers to the development of basic space sciences and the promotion of space knowledge, space technology, and space achievements among young scholars. It also specifically addresses a number of policy issues for national space security, the most important of which are:

- Consideration of regional and international defense treaties and, if necessary, accession to them.
- Effective membership in regional and international defense organizations within the framework of foreign policy and based on national security priorities.
- Recognizing space threats ahead and methods of dealing with them.
- Improving collaboration with universities or industries and integration of aerospace defense networks.
- Improvement and development of indigenous and national standards of space strategic systems in products and services and increasing their reliability and intelligence (Islamic Republic of Iran 2013).

## **The Five-Year Iranian Economic, Social and Cultural Development Plans**

The Five-Year Iranian Economic, Social and Cultural Development Plans (Five-Year Development Plans) are known as a set of interim plans, which are prescribed by the state for 5 years and approved by the Parliament. Six development plans have been

approved after the Islamic Revolution of Iran in 1978. Since 2004, by regulating the Fourth Development Plan Act, aerospace and space security activities have also been considered. The focus on space industry and activity in development plans is actually the explanation of high-level national documents such as the Vision Plan, the Comprehensive Scientific Map of Iran, and the Comprehensive Document of Aerospace Development for 5 years (Islamic Republic of Iran 2013).

### **The Fourth Development Plan Act**

The Fourth Development Plan Act was approved by the Parliament in 2004 (Islamic Republic of Iran 2004). The state is obliged to make necessary schemes for the extreme exploitation of national and regional capacities in the aerospace sector with regard to the importance of knowledge role, technology, and ability as the main factors of value added in recent economy. Moreover, according to the Act (Islamic Republic of Iran 2004), the state should promote new or emerging technologies and data applications in utilizing defense systems. They should be made to strengthen defense and military capabilities of the state in order to protect security, territorial integrity, national or vital interests, and resources of the country in preparing against any threats. As it can be seen, the Act does not specifically address space high-level policies and strategies. But it has directly obligated the state to apply and develop national and regional aerospace capabilities (Islamic Republic of Iran 2004).

### **The Fifth Development Plan Act**

The Fifth Development Plan Act was approved by the Parliament in 2011 and has significant arrangements in the space domain. The Act declares (Islamic Republic of Iran 2011b, January 5) that the state may take necessary steps to create and develop infrastructure related to designing, operating, and testing space satellite systems, ground station, and satellite launch vehicle due to the ever-increasing importance of the space sector and achieving new or emerging technologies to ensure required space applications and services in Iran. In addition to that, it explains that the state should maintain orbital slots for Iran and predict approaches so as to establish the infrastructure and implement national satellite projects to protect such slots.

In terms of defense and security, it refers to the establishment of command, control, data, and advanced supervision systems in different aspects including space, air, sea, and land in order to promoting awareness and being prepared to recognize threats and taking measures to encounter them effectively (Islamic Republic of Iran 2011b, January 5). It seems that the Act comparing to other national space-related law and regulations is unique, because as a high-level national document, it not only sets general requirements in the field of space activity development but also has posed specific tasks on the state, such as preserving national orbit slots.

### **The Sixth Development Plan Act**

The Sixth Development Plan Act has been approved in 2017 (Islamic Republic of Iran 2017). It has prioritized the space sector, and it considers the development of space activities. In the General Policies section of the Act, first it refers to prioritizing

industrial strategic areas such as aerospace and increasing the technology influence, and then it addresses the development of space technologies (Islamic Republic of Iran 2017, paragraphs 28 and 38 of the General Policies section). All these policies are detailed in the Act (Islamic Republic of Iran 2017, Article 40), according to which, the state is obliged to take the following steps in order to develop air and space industry and acquire new science and technology in that field:

1. The necessary support for the development of infrastructure and industries related to the designing, manufacturing, testing, and operation of space systems, satellite launch vehicles, satellite, and ground stations.
2. Maintaining orbital slots which belong to Iran and also predicting necessary arrangements to establish and implement national satellite designs so as to maintain the aforementioned slots (Islamic Republic of Iran 2017, Article 41).

Obviously, the strategy, policy, and fundamental measures for space activities are dealt within the Act. Regarding the space strategy, it provides for a balanced development of activities the highest utilization of space infrastructure and also the maintenance of orbital slots. In the field of policy making, the Act states:

- Utilizing the full capacity of domestic space actors and transfer of advanced technologies along with maintaining systematic integration of capabilities.
- Cooperating with foreign space operators and manufacturers.
- Cooperating with the nongovernmental sector (national and foreign) in order to purchase national satellites.

Concerning fundamental measures, the state is expected to manufacture telecommunication satellites, remote sensing satellites, and to purchase national satellites. In the Act, a separate section is devoted to the science and technology in the space industry. This section focuses on designing, manufacturing, testing, operating, and deploying space systems and maximizing the maintenance and utilization of orbital slots in national space policy so as to provide development opportunities for Iran's space technology (Islamic Republic of Iran 2017, Article 42). The quantitative objectives for the development of space activities in the Act can be seen in Table 3:

### **Supervisory and Regulatory Structure for Implementing Space High-Level Policy Documents**

There are two important regulatory bodies regarding the implementation of space policies set forth in the high-level space policy documents in Iran: the Supreme Space Council and the Iranian Space Agency. Until 2003, there was no dedicated institution for space activities in Iran. In that year, the Parliament established the Supreme Space Council, chaired by the President and the relevant space entities who are members. In the same year, the decree of the Iranian Space Agency was approved. According to the Comprehensive Document of Aerospace Development

**Table 3** Quantitative objectives of Sixth Plan in the space domain

General objective	Quantitative objective		Status at the end of year 2015	Years of Sixth Plan				
	Subject	Unit		2016	2017	2018	2019	2020
Increase the level of technology, infrastructure, space applications, and utilization or maintenance of orbital slots for a country	Increase the capability of national technology, manufacturing remote sensing satellite, and telecommunication satellite to 50%	Percent	1	5	15	25	35	50
	Purchase and operate two telecommunication and remote sensing satellites	Number	-	-	1	2	-	-
	Offer 15 new space services considering value added	Number	-	2	4	7	11	15

approved by the Supreme Council of the Cultural Revolution, the Supreme Space Council is the highest policy-making authority in the space domain of the country and has responsibilities to execute, lead, supervise, and approve major space-based plans and strategies. The Statute of Council was approved by the Cabinet in 2004 (Ataafar 2009). The Supreme Space Council is responsible for the policy making and for determining the general outline within which the space activities regime in Iran is developed. The Iranian Space Agency is responsible to implement the policy developed by the Supreme Space Council. Since the decision of the latter is inclusive and has both domestic and international policy dimensions, the obligations of the Iranian Space Agency are also comprehensive. Although the Iranian Space Agency manages the governance of the development of space technology and space activities for peaceful purposes, it should be noted that universities and aerospace research institutes practically develop space science and technologies in Iran (Ataafar 2009).

### **Challenges on Implementing High-Level Iranian Space Policy Plans and Documents**

The aforementioned high-level documents on space activities have been regulated and approved by the responsible authorities. According to the Vision Plan, space defense and security capabilities and technology policies should be defined and regulated. Therefore, various documents on air and space fields have been approved according to this key document. Alongside the Vision Plan conveyed by the Supreme Leader, other high-level documents such as the Comprehensive Scientific Map and the Comprehensive Document of Aerospace Development are approved by the Supreme Council of the Cultural Revolution. These high-level documents contain elements for strategy and policy making adopted by the competent authorities to achieve specific goals or obtain appropriate means for those purposes. The documents are implemented by the various executive entities and can be enforced by the legislator if necessary.

Most of the governmental and nongovernmental agencies are facing challenges concerning the specific legal status and the implementation of the mentioned documents. Generally, these documents contain program elements that are in the form of guidelines, meaning that they do not have the content and legal status of the documents or programs approved by the Parliament or the Cabinet. In fact, these documents lack the necessary binding status and are mainly used to guide the formulation of government development plans approved by the Parliament. Iran has attempted to regulate its long-term policies and programs in these documents in various domains, including space activities. In the space sector, however, non-allocation of funds or deviation of priorities in scientific, economic and technological aspects can affect the goals set out and their implementation. The implementation of such documents generally depends on various political and economic conditions. Besides, the Parliament or the Cabinet shall approve the relevant regulations for the government agents to find a legal way to accomplish the purposes thereof.

Two important factors are added to the emerging challenges of implementing these documents in the space domain:

1. Iran's space activities face a lack of integration. An integration of space activities and organizational integrity should be considered in these documents. There are various space institutions in Iran, including executive, scientific, and technology related that are involved in implementing the high-level space policy documents. However, it is not legally clear which entity is responsible to apply what part of the policy. The responsibilities of any military, governmental, and non-governmental entity in the conduct of space activities should be clearly stated. There is a need that space policy documents outline that the responsibilities of institutions and authorized entities based on research, scientific, and technological requirements.
2. Besides the necessity of codifying regulations to specify the tasks of each space entity, it is also required to create a coherent structure to apply and control high-level space policies. Although according to law, the Iranian Space Agency and the Supreme Space Council are responsible to implement the document of Aerospace Development, to determine main authorities, and to consider priorities in the allocated budget, they have not succeeded in the process. Firstly, the Supreme Space Council has rarely and disorderly convened since its establishment. Secondly, the Iranian Space Agency has administrative activities that have prevented it to fulfill its sovereign responsibilities. Thirdly, Iran has not yet approved a national space law. Codifying such law could facilitate the way for governmental and nongovernmental institutions to engage in space activities. According to the provisions of national space law, organizations, private companies and individuals could access their position in implementing high-level national space policy documents.

---

## **A Glance at the Space Security of Iran**

Outer space plays a pivotal and determining role in ensuring the security of countries and international community. Space security is recognized as one of the most fundamental components of relations among countries. Therefore, countries tend to set long-term goals in order to expand their space activities. The balance of power constitutes the main reason which may result in security challenges in space. The arms race in space might create benefits or hindrances to the balance of power. The balance of power is a major phenomenon brought about by the structure of an international system relating to the external behavior of countries. By the end of bipolar order between the two countries, the USA and the former Soviet Union, space age entered into a new phase providing an opportunity for new space farers to participate in space activities. Along with the continued traditional use, namely, research, military, and quasi-military, the use of space expanded to commercial and civilian activities, with both governmental and nongovernmental actors particularly



in the development of communication, commercial, and telecommunication satellites (Moltz 2019).

Given the mentioned circumstances, Iran has decided to introduce itself as a new space-faring nation. Iran's approach to regulating space is transparent. International peace and security is very important to Iran. Iran desires to gain the benefits that space technology has brought to other space-faring nations. It has gradually developed its presence in space activities over the past two decades and continues to do so by taking steps forward. The expansion of space activities with the acquisition of advanced space technology in recent years has positioned Iran among countries that actively participate in outer space activities. Iran is one of the new space actors which could develop the capability to launch its satellites and sounding rockets and eventually join the few space-faring nations that have accessed space (UNCTAD 2016).

There was no organized structure in the space policy of Iran till 2004. The establishment of the Iranian Space Agency in 2004 enabled Iran to systematically develop space activities in the different fields of communication, telecommunication, remote sensing, meteorology, geology, exploitation, and so on. The launch of the Omid satellite could mark Iran's engagement with the development of a space industry. Aiming to expand its space activities and its presence in outer space, Iran space policy includes the commercialization of space applications, Earth observation and environmental changes, mapping and weather forecasting, as well as the promotion of international cooperation and the involvement of private entities. Therefore, it can be said that space policy in Iran was based on crucial steps especially in terms of designing and manufacturing of satellite (Malmiran 2009).

Although Iran's space activities are just beginning, they exert positive influences on Iran's space security policy at national and international level. The space security policy of Iran revolves around four themes:

1. At international and national level, Iran has always emphasized the peacefulness of space activities carried out by Iran or other countries. Iran has signed four of the United Nations treaties on outer space. The space policy of Iran is actively being developed at all international and regional meetings related to space subjects, including space security (Zargar 2010).
2. Iran, since the establishment of UNCOPUOS in 1959, views international cooperation as central to space security. In the 1970s, the pursuit of space activities and the development of satellite communications were considered important for Iran. Iran is one of the 65 members in the Conference on Disarmament (CD) which supported the "Prevention of an Arms Race in Outer Space." This approach of Iran has shown its attention to outer space and space technologies, despite the fact that the country didn't have space activity back then. Iran plays an important role in the strategic cooperation for outer space activities in Asia and is also a member of the Asia-Pacific Space Cooperation Organization (APSCO) for multilateral cooperation in technology and space applications along with China, South Korea, Thailand, Bangladesh, Indonesia, Peru, and Mongolia. Iran is also a member of the Islamic Space Science and Technology Network (ISNET) (Khosravi et al. 2013).

3. Iran seeks to develop its space activities in accordance with official aerospace strategic documents that have been developed within the last two decades. As stated above, it aims to codify a strategy that assures space security within its national policy. According to the provisions of high-level national space policy documents, the access to space through the active presence of Iran has been recognized as an essential matter in line with Iran's national interests. Iran intends to achieve the first place in economic, scientific, and technological fields such as space in the Middle East. In the development plans of the country, producing space science and access to new space technologies is one of the top priorities (Gorwitz 2011).
4. Iran has affirmed the exploitation of space to ensure Iran's security by reducing threats and using space to defend the country's territorial integrity and enhance its positioning. Iran also seeks to develop space activities for peaceful purposes among which operating meteorological satellites are the examples. In 2009, the Fourth Development Plan Act was codified in which the highest importance was placed on space technology applications as an effective means for the sustainable development of the country. Based on the Act, there is a need of acquiring space science and technology as well as cooperation with the international community (Kamran and Nami 2008).

---

## Conclusion

The development of space technologies has made available various space applications in remote sensing, communications, telecommunications, earth observation, use and exploitation of celestial bodies, and so forth. Moreover, due to the expansion of space technology, the number of space-faring nations has been increasing far beyond the initial few countries with the involvement of many new countries entering the space industry. There has also been a surge in the number of private entities that engage in space activities. Iran has increased its space activities over the last couple of decades. At the same time, policy makers and legislators have approved Iran's space policies and strategies aiming to regulate space activities. Pursuant to the Constitutional Law, the long-term space policies of Iran have been codified in the "Vision Plan," followed by the "Comprehensive Scientific Map" and the "Comprehensive Document of Aerospace Development." The aerospace policies of the country have been enacted and implemented under the Five-Year Development Plans as well.

Iran's space policy is also reflected in its international presence. At international level, Iran's approach is not only to ratify and enforce international space treaties but also to maintain an active presence in UNCOPUOS and an effective role in determining resolutions and guidelines issued in the form of soft law. Iran also desires to expand its international cooperation with other countries through multilateral, regional, and bilateral agreements on space activities, especially in space science and research. The same approach to international cooperation applies also to space security and space defense as explained in Iran's space security policy. The peaceful

use of outer space has always been highlighted in Iran's policy on space security as reflected on the development of space science and research. Firstly, the emphasis is on designing, manufacturing, producing, and operating national satellites for various peaceful uses. Secondly, human presence in space is declared as a feature of national autonomy. The development of space technologies and activities aimed at defense affairs for countering probable cyber and space attacks, are emphasized by the national security policy.

---

## References

- Ataafar A (2009) Vision of development and fundamental revolutions required for universities. *Iranian Higher Education Quarterly*, no 4, 1st year, at 27
- Blount PJ (2010) The development of international norms to enhance space security law in an asymmetric world. *Proceedings of the 52nd Colloquium on the Law of Outer Space*, p 2
- Bockel JM (2018) The future of the space industry, NATO Parliamentary Assembly, General Report 173 ESC 18 E fin | Original: French | Available at: <https://www.nato-pa.int/>
- Concini A, Toth J (2019) The future of the European space sector How to leverage Europe's technological leadership and boost investments for space ventures, European Investment Bank. Available at: [https://www.eib.org/attachments/thematic/future\\_of\\_european\\_space\\_sector\\_en.pdf](https://www.eib.org/attachments/thematic/future_of_european_space_sector_en.pdf)
- Global Security (2010) In 1997, Iran made plans to develop satellites called Mesbah (Lantern). Available at: [GlobalSecurity.org. http://www.globalsecurity.org/space/world/iran/multi.htm](http://www.globalsecurity.org/space/world/iran/multi.htm)
- Gorwitz M (2011) Iranian dual-use space related research, Iranian dual-use science and technology bibliography, vol VII, Space Related Research. Available at: <https://fas.org/nuke/guide/iran/biblio5.pdf>
- Harvey B, Smid HHF, Pirard T (2010) *Emerging space powers. The new space programs of Asia, the Middle East and South-America*. Springer
- Islamic Republic of Iran (1989) Iranian constitutional law 1989. Article 110
- Islamic Republic of Iran (2003) The Vision Plan of Iran by 1404 (2024), approved in 2003 November 4. Available at: <https://rc.majlis.ir/fa>
- Islamic Republic of Iran (2004) The Fourth Economic, social and Cultural Development Plan Act, approved by Parliament in 2004 September 1. Available at: <https://rc.majlis.ir/fa>
- Islamic Republic of Iran (2011a) The Comprehensive scientific map of Iran approved by Supreme Cultural Council of the Islamic Republic of Iran in 2011 January 4. Available at: <http://www.nlai.ir/documents/>
- Islamic Republic of Iran (2011b) The Fifth Economic, Social and Cultural Development Plan Act by 2012–2016, approved by Parliament in 2011 January 5, no 73285/419. Available at: <https://rc.majlis.ir/fa>
- Islamic Republic of Iran (2013) The Comprehensive document of aerospace development approved by Supreme Cultural Council of the Islamic Republic of Iran in 2013 January 8, no 728. Available at: <http://www.nlai.ir/documents/10184/198216/>
- Islamic Republic of Iran (2017) The sixth Economic, Social and Cultural Development Plan Act by 2018–2022, approved by Parliament in 2017 March 4, no 20995 RooznamehRasmi. Available at: [www.dastour.ir](http://www.dastour.ir)
- Kamran H, Nami MH (2008) Space, power, security. *J Iranian Geogr Soc* 16, 17, 6th year. Available at: <http://ensani.ir/>
- Khosravi I, Joday J, Jafari SA (2013) Impacts of armed arena on military security of Islamic Republic of Iran. *Defense Policy Magazine* 22(85). Available at: [https://journals.ihu.ac.ir/article\\_203188.html](https://journals.ihu.ac.ir/article_203188.html)

- Malmiran H (2009) Space, technology and its role in National Security of Islamic Republic of Iran. *Strateg Stud Q* 26:149–174. 7th year
- Moltz JC (2019) *The politics of space security; strategic restraint and the pursuit of National Interests*, 3rd edn. Stanford University Press
- Tarikhi P (2009) Iran's space program: riding high for peace and pride. *Space Policy*, at 3
- Tarikhi P (2015) *The Iranian space endeavor, ambitions and reality*. Springer, Cham, pp 140–141
- UN Treaties. United Nations Treaty Collection. Outer Space. Note Table 1 and also Table 2. Available at: [https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&msgid=XXIV-2&chapter=24&clang=\\_en](https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&msgid=XXIV-2&chapter=24&clang=_en)
- UNCTAD (2016) United Nations conference on trade and development. Science, technology and innovation policy review – Islamic Republic of Iran, United Nations publication UNCTAD/DTL/STICT/2016/3. United Nations. Switzerland. Available at: [https://unctad.org/en/PublicationsLibrary/dtlstict20163\\_en.pdf](https://unctad.org/en/PublicationsLibrary/dtlstict20163_en.pdf)
- Zargar A (2010) Space and National Security; Iran's space developments enhancing National Security. *Foreign Policy Q* 3. Available at: [http://fp.ipisjournals.ir/article\\_9512.html](http://fp.ipisjournals.ir/article_9512.html)



Naser Al Rashedi, Fatima Al Shamsi, and Hamda Al Hosani

## Contents

Introduction .....	622
The Importance of Space to the UAE .....	623
National Regulatory Framework for the UAE Space Sector .....	625
The UAE's Contribution to International Space Cooperation .....	627
The UAE Space Economy .....	628
The UAE Contribution to Sustainability .....	629
The UAE Space Strategy's Contribution to Space2030 Agenda .....	629
The UAE Space Sector's Contribution to the 17 SDGs .....	634
The UAE Space Policy Contribution to the LTS Guidelines .....	642
LTS Guideline A: Policy and Regulatory Framework for Space Activities .....	643
LTS Guideline B: Safety of Space Operations .....	645
LTS Guideline C: International Cooperation, Capacity-Building, and Awareness .....	646
LTS Guideline D: Scientific and Technical Research and Development .....	649
Conclusions .....	650
References .....	651

## Abstract

Space exploration and utilization have been able to enrich the human knowledge of the universe and contribute to facilitate and improve the daily lives of humans in different aspects, such as communication, earth observation, weather, and navigation. The leadership of the UAE has realized the increasing importance of the space sector and supported its continuous growth at a regional and global level.

Due to the increasing number of activities in the space industry, and dependency on the space applications, as well as the growing rate of national investments, combined with the technical, economic, and political developments in the sector,

---

N. Al Rashedi (✉) · F. Al Shamsi · H. Al Hosani  
Space Policies and Legislations Department, UAE Space Agency, Masdar City, Abu Dhabi, United Arab Emirates  
e-mail: [N.alrashedi@space.gov.ae](mailto:N.alrashedi@space.gov.ae); [F.alshamsi@space.gov.ae](mailto:F.alshamsi@space.gov.ae); [H.Alhosani@space.gov.ae](mailto:H.Alhosani@space.gov.ae)

the UAE government decided to further consolidate, and grew these into a sustainable national space program; and establishing a federal authority to oversee, support, and promote the space sector in the UAE.

The UAE Space Agency is focused on establishing a national space policy and regulatory framework, building national human capacity in various space professional fields, supporting R&D, expanding national space activities, and strengthening national and global partnerships to support the space program and sector. Moreover, the Agency actively works towards increasing and spreading the use of space technology and applications in the UAE, with aim of maximizing the benefits from them towards other sectors needs and national interests. As such, the agency helps the nation achieve its diversification plans and supports the creation of a knowledge-based economy. The UAE actively contributes in utilizing space to achieve long-term sustainability. In line with this mandate, the UAE National Space Strategy 2030 has been reviewed to ensure its alignment with the 17 Sustainable Development Goals (SDGs), the Long-Term Sustainability Guidelines, and the four pillars defined in the revised zero draft of the “2030” Agenda.

In this chapter, the UAE is proud to show the strong and diverse space sector, which over the past three decades managed to develop capacities and expertise qualifying it to compete globally and to move on to a new era in its national space program.

---

## Introduction

Outer space refers to the expanse starting around 60 miles from the Earth’s surface and reaching the other celestial bodies. It is made of a hard vacuum and contains low-density particles, mainly the plasma of hydrogen and helium. Besides that, outer space is a source of electromagnetic radiation, magnetic fields, cosmic rays, and a number of other elements that can pose threats. Nonetheless, space activity refers to any kind of human-carried activity in outer space.

It has been more than six decades since the Soviet Union launched the first satellite Sputnik 1, which marked the start of space activities for various purposes, including communication, scientific experiments, military uses, navigation and global positioning, and intelligence gathering, just to name the few. As the time passes, a vast majority of countries are becoming progressively more dependent on global satellite capabilities for national and international infrastructures. Without satellites, it would be impossible to achieve routine tasks such as airspace and ships’ navigation, financial transactions, as well as to reap the benefits of modern telecommunications and the Internet. Hence, satellites have become essential tools, enabling social, economic, and scientific activities and bolstering private and public sectors’ infrastructure. Outer space recognizes no concept of national borders, allowing all countries not only to utilize satellites for different purposes but to also work on boosting satellites’ capabilities (Outer Space and Security (2014)).

Nevertheless, outer space is considered to be the most fragile system that exists due to its limited ability of self-recovery. Near-Earth space, which is the atmosphere, is the only known part of the outer space being able to take out satellites from orbit, while the objects stuck in the proximity of more than 800 km from the atmosphere will remain in the position for hundreds of years. Due to the ever-increasing volume of space activity, and resulting space debris, “near-Earth space” requires proper attention and protection for the benefit of all humankind (Moltz 2002).

Events such as deliberate destruction of obsolete satellites or other space objects without the consent of the other countries could further increase the amount of debris and pose a significant threat to the integrity of other satellites. One such event took place in 2007 when China conducted ASAT (anti-satellite test) to destroy one of its satellites. That event corroborated even further the need for stable use of the outer space and highlighted the critical challenges that can emerge for space activities (Issues in the International Community 2014). Similar activity was also conducted by India in March 2019, when launched the Ballistic Missile Defence, Interceptor missile, in ASAT missile test (Mission Shakti) engaging an Indian orbiting target satellite in Low Earth Orbit (LEO), and consequently turning the object into debris.

It is noted, however, that the first steps for outer space protection have been defined in the Outer Space Treaty of 1967. The treaty states that the exploration and use of outer space, including the moon and other celestial bodies, should be only conducted for the benefit of all peoples regardless of their economic or scientific development. On top of that, it encourages free access to all areas of space for all countries, as well as international cooperation, while it forbids the use of outer space for installation of any kind of weapons of mass destruction. Furthermore, it proclaims all States members bear responsibility for national space-related activities carried out by either governmental agencies or nongovernment entities. Also, each State Party to the Treaty that launches or procures the launching of an object into the outer space is liable for damage to another State Party (Outer Space Treaty of 1967 n.d.).

Ever since the launch of the first satellite, there has been an ever-increasing competition in space activities between developed nations. Moreover, influence and participation in space activities reflect an element of governmental power for these nations. In turn, this leads to the increasing interest for participation and investment in space activities among emerging and developing nations. Nowadays, there are more countries willing to invest in space activities than ever before.

---

## **The Importance of Space to the UAE**

Space utilization and discoveries have been able to enrich the human knowledge of the universe and contribute to improving the daily lives of human beings. As such, communication, broadcasting, earth observation, and navigation applications using satellite data contribute remarkably to the conduct of daily human activities. In addition, space technology supports vital societal services and sectorial policies.

Moreover, the use of space-based assets plays a vital role in monitoring the weather, climate and environmental change, management of natural resources, crises

and disaster management, as well as rescue and humanitarian aid programs. Also, many capacities and advanced technologies that were developed for space have been widely used in other domains such as medicine, energy, and manufacturing. Hence, the space sector has become a source of innovation and inspiration for human beings and, particularly, for the generations to come.

The good leadership of the United Arab Emirates (UAE) has realized the increasing importance of the space sector and its continuous growth at a regional and global level. This is why it has been investing in space since the early 1990s. Today the UAE is proud to have a strong and diverse space sector. The UAE has managed over the past three decades to develop space capacities and expertise qualifying it to compete globally and to move on to a new phase in its national space program. Thus, in 2014, the UAE Space Agency was created and the UAE Mars exploration program was announced.

Provided the increased national investments and growing activities in the field of space, combined with the technical, economic, and political developments in the space industry, the UAE government aims at establishing a national policy and regulatory framework for space activities. Such intention follows suit the international developments and is aligned with the UAE government's ambitions and higher interests that have manifested in the national agenda of the UAE Vision 2021 and Centennial 2071. The latter are aimed at enhancing the role of the space sector and, thereby, making the UAE among the best countries in the world with a stable and diverse economy providing for current and upcoming Emirati generations. This entails the transition toward a knowledge-based economy centered on innovation, high-level education, and increasing national expertise and qualifications.

Since its establishment, an annual budget is assigned to the UAE Space Agency by the UAE Federal Cabinet with the aim to improve the lives of its citizens, national security, crisis management, discovery of national resources, climate monitoring, diversification of the UAE economy, and further strengthen cooperation with the other States. In 2017, the UAE Space Agency made an agreement with Luxembourg on cooperation and exchange of information and expertise in the areas of space science, research, and technology (The Economic Times 2017). In addition, the UAE has taken a part in international cooperation initiatives for space activities led by China. As a matter of fact, the UAE has become part of "the Belt and Road" initiative and has consequentially become integrated in China's space-based infrastructure services, such as BeiDou Satellite Navigation System, satellite communications, and remote sensing (Hui 2018).

The UAE has also become a part of the "International Charter Space and Major Disasters." Moreover, the Mohammed Bin Rashid Space Centre has joined Sentinel Asia with the goal of supporting disaster management in the Asia-Pacific region by means of providing high-resolution satellite images. In November 2016 and 2017, in partnership with UNOOSA, the UAE held the High Level Forum on using space as a driver for sustainable development and signed an agreement on the peaceful uses of outer space (Space Security Index 2019).

The UAE has also become the first Arab country to fully manufacture its own satellite, KhalifaSat, which is one of the most advanced remote sensing satellites,



allowing the UAE to establish its position on the global map of space activities (MBRSC 2019).

---

## **National Regulatory Framework for the UAE Space Sector**

As per the UAE Federal Decree No. 1 of 2014, the UAE Space Agency has the mandate of overseeing and promoting the country's space sector and activities. Under such mandate the agency is responsible for the development of the so-called "National Space Framework" consisting of four main components, namely, Space Policy, Space Strategy, Space Law, and Space Regulations.

In 2016, the agency launched the National Space Policy, which clearly states the UAE principles and ambitions for its space program. The policy addresses the reasons that the UAE is investing in space and what the ultimate goals are. It consists of six main sections that summarize the importance of outer space and explain the main purpose of the policy. It also explains how the space sector will contribute to the achievement of the national vision, priorities, and goals and defines the capabilities, guidelines, and governance system needed to support the achievement of the policy goals.

In March 2019, the National Space Strategy 2030 was approved, setting the general framework for the UAE's space industry and activities carried out by public and private entities for the years leading up to 2030. Following the Cabinet approval, the UAE Space Agency launched the National Space Strategy 2030, which translates the principles and ambitions in the policy into a set of national programs and initiatives to be implemented by the United Arab Emirates space sector by the year 2030. The UAE throughout the 18 programs of the National Space Strategy will work on achieving 71 initiatives. The strategy is structured around six strategic objectives, namely, competitive and leading space applications and services, advanced R&D and manufacturing capabilities, inspiring space scientific and exploration missions, high level of space awareness and expertise, effective local and international partnerships and investments, and adopting and enabling frameworks and infrastructure.

In December 2019, the National Space Law was approved and came into effect, hence setting the regulatory basis for space activities by covering the organization and objectives of space projects undertaken by the country, including peaceful space exploration and the safe use of space technologies. It also addresses new and complex concepts, such as the right to own resources found in space and organizing manned space travel and other commercial activities, such as asteroid mining.

Also, the Space Investment Promotion Plan aims to achieve these Policy directions by defining in a high level the UAE approach to facilitate more investments in space industry in the UAE, and contribute towards the attainment of UAE goals stated in the UAE Vision 2021, the UAE 2071, and the UAE Plan on the 4th Industrial Revolution. In particular to diversify and ensure sustainability of the UAE Economy; to promote highly productive knowledge-based economy; to provide incentives for R&D and innovation, and to encourage entrepreneurship and

SMEs role and opportunities in private sector. The Space Investment Promotion Plan is structured around four objectives:

1. Sustain the growth of the UAE Space Industry.
2. Increase the UAE space sector contribution to the diversification of national economy, and to knowledge-based economy.
3. Support other national strategic interests.
4. Promote partnerships at national and international levels.

The plan is further supported by two complementary pillars allowing UAE to propose a desirable and unique offering for Early- and Later-Stage space companies looking for VC funds compared to other locations worldwide. The first pillar is on creating an attractive environment for space industry and ecosystem, whereas the second pillar is on creating an investment vehicle and the need supporting entities through setting up a catalyst, then a platform to facilitate investment, creating UAE Space Angels to invest in seeds, and in creating Space Accelerator to help start-ups and entrepreneurs. Additionally, to support and enable the space sector, in 2020, the UAE Space Agency developed and approved the Remote Sensing Space Data Policy Guidelines for Institutional UAE Missions, where it:

1. Recalls principles, goals, and ambitions stemming from the UAE National Space Policy and elaborates these in the context of UAE Institutional RS space missions and data provision.
2. Contains voluntary guidelines that aim at providing a reference to UAE Institutional RS space mission owners/operators to develop their own data policies for their own missions.

These data policy guidelines leverage international best practices and include forward looking considerations. They have been developed for RS Institutional (civil or dual-use) satellite missions generating remote sensing data. They provide guidance to UAE RS institutional satellite owners/operators to develop their own data policies. Whenever meaningful, each main data policy topic is addressed in these guidelines by providing a best practice characterization from both an Open and a Restricted data policy approach. An UAE RS institutional satellite owner/operator reading these guidelines should be able to clearly see which data policy approach is most suitable to its mission(s) and find useful references that can be of assistance, or inspiration, in shaping its own data policy. A data policy always needs tailoring to the specificities of a given mission and its owner/operator objectives. Furthermore, the UAE Space Agency is working towards establishing a comprehensive legal framework and principles to regulate the national space sector, which aims to clearly define the requirements and the legislation for conducting space activities and the activities supporting the space activities in the UAE. Hence, the Agency is currently working in drafting a set of regulations and guidelines including the following: Regulation on Authorization of the Space Objects, Regulation on Registration of the Space Objects, Regulation on Human Spaceflight Activities, Space Debris Mitigation Guidelines, and Third Party Liability Insurance Guidelines.

## The UAE's Contribution to International Space Cooperation

The United Arab Emirates acknowledges the significance of supporting international cooperation in the field of exploration and peaceful uses of outer space. This comes with placing importance on strategic discussions at international level that ensure aligned directions toward achieving the common goals.

With the aim to accelerate the dialogue on the role of space science and technology in achieving global development, the first High Level Forum (HLF) was held in Dubai, United Arab Emirates, during the period of 20 to 24 November 2016. The event was co-organized by the United Nations Office of Outer Space Affairs and the government of the United Arab Emirates. The forum provided a platform for the space community to exchange recommendations for the UNISPACE+50 blueprint and to share insights in regard to the global governance and the role of space science and technology in supporting the achievement of the global sustainable development in each of the four thematic pillars identified by the office, namely, space economy, space society, space accessibility, and space diplomacy.

The United Nations/United Arab Emirates High Level Forum resulted with the Dubai Declaration, which recommended the forum to continue to serve as a platform for the space community to exchange views on connecting the four pillars of the UNISPACE+50 and Space2030 and to encourage collaboration with the United Nations Office of Outer Space Affairs. There were a number of discussion sessions addressing the following (United Nations/United Arab Emirates High Level Forum: Space as a driver for socio-economic sustainable development 2017):

- The importance of coming up with solutions addressing the need to guarantee access to space and the availability of a regulatory instrument mechanism for cooperation to ensure benefits for global societies
- The achievement of goals set by the 2030 Agenda for sustainable development with the support of space and its role as a driver for social and economic sustainable development
- The importance of joining global efforts in the development of space, taking various aspects into account, such as space technology data and facilities
- The role of regulatory frameworks and international mechanisms at the national and international level in achieving cooperation in the peaceful exploration and use of outer space

In June 2018, the international community gathered in Vienna for UNISPACE +50, a special segment celebrating 50 years after the first United Nations Conference on the Exploration and Peaceful Uses of Outer Space during the 61st session of the Committee on Peaceful Uses of Outer Space (COPUOS). It offered an opportunity for the international community to agree on the upcoming steps toward better global space cooperation for the benefit of mankind.

The UAE followed the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) endorsement for the UNISPACE+50 resolution “international cooperation in the peaceful uses of outer space,” which was adopted by the General Assembly on 7 December 2018. The United Nations resolution A/RES/73/91 called

for “strengthened international cooperation in the peaceful use of outer space and the global governance of outer space activities, and encouraged coordination to ensure that space science, technology and applications serve the Sustainable Development Goals.” The resolution represents affirmation by the global community of the critical role that space can play in attaining the UN Sustainable Development Goals (SDGs) and moreover, of the needed for collaboration and partnerships at all levels in order to expand the opportunities and maximize and reap the benefits space could provide in this regard.

Therefore, the UAE government played a significant role in the preparation of the UNISPACE+50 and the development of the above remarkable UN resolution. The continued efforts of the UAE comes from its deep value and recognition of the essence of space and its significant impact on improving everyday lives, as well as its role in general as a driver for the socioeconomic sustainable development of the country, the Arab region, and the world as a whole.

---

## The UAE Space Economy

It’s worth noting that the UAE space sector has accomplished a number of significant developments at national, regional, and international levels. Most of those achievements were enabled by the continuous process of regulation and organization of the sector by the UAE Space Agency toward achieving its strategic goals. Besides, the UAE Space Agency is focused on raising national capabilities and the use of space technology in the UAE. As such, the agency helps the nation achieve its diversification plans and supports the creation of a knowledge-based economy.

What is more, the UAE has developed the most diverse space sector in the Middle East and North Africa (MENA) region, thus, representing a regional hub for space activities, services, technology, education, and events. Its sector consists out of over 52 entities contributing to the space economy, including six main players, namely, the UAE Space Agency, the private entity YahSat/Thuraya, the National Space Science and Technology Center (NSSTC), Mohammed Bin Rashid Space Centre (MBRSC) Sharjah Academy of Astronomy, Space sciences & Technology (SAASST), and Khalifa University. One of the UAE’s most ambitious missions, as well as the first of the kind in the region, is the Mars exploration mission, named “The Hope” (Building UAE Space Capabilities 2017).

When it comes to measuring the socioeconomic impact of the space industry, the space economy survey has been developed and conducted in partnership between the UAE Space Agency and the Federal Competitiveness and Statistics Authority since 2018. The purpose of the survey was to collect data meant to measure the National Agenda indicators in accordance with the UAE Vision 2021, and the UAE Centennial 2071, as well as a number of sectorial and strategic Key Performance Indicator (KPIs) concerning the space sector. The survey methodology followed best practices adopted by OECD. The following parameters have been analyzed: the contribution of the space sector to the UAE economy, the total number of staff employed in the

UAE space sector, expenditures on the UAE space sector, and expenditures on research and development (R&D) in the UAE space sector.

The survey provides important data for decision-makers in the country to take the appropriate action regarding monitoring and enhancing the competitiveness of the UAE space sector. The study indicates positive trends in expenditures on R&D and space exploration, where 38% and 63% increases have been recorded on the expenditures of the R&D and space exploration assets, respectively. Moreover, the study shows 41% increase in expenditures on commercial projects in the space sector, as well as significant increase in the percentage of women working in the 12 national space operators, which totaled 47% at the time when the study was conducted. Ultimately, the average community awareness of national space institutions is estimated at 65%, whereas awareness among students has been reported to be significantly above the average, equating to 81%.

---

## **The UAE Contribution to Sustainability**

### **The UAE Space Strategy's Contribution to Space2030 Agenda**

In 2015, the world leaders adopted the 17 Sustainable Development Goals and their objectives for the sustainable development plan for 2030 (SDGs). It is worth mentioning the important role of the UAE in supporting these objectives and the role that space applications and services can play in achieving a number of these goals. Accordingly, in January 2017, the National Committee on SDGs was formed by the UAE Cabinet Decree No. 14 of 2017. The committee was chaired by Her Excellency Reem bint Ebrahim Al Hashimy, Minister of State for International Cooperation, and the Federal Competitiveness and Statistics Authority serving as vice chair and secretariat. As of 2018, the committee includes 17 members, which is led by FCSA and includes federal government entities, working toward the successful implementation of the SDGs. The mandate includes:

- Aligning the SDGs with the UAE's national development priorities and serve as a coordination body to implement the SDGs
- Undertaking regular follow-up and review of progress on implementation
- Managing domestic and international stakeholder engagement
- Coordinating the collection of official statistics, identifying new data sources, and assisting the National Statistics System to build capacity to monitor and report on SDG indicators
- Managing ad hoc SDG-related projects assigned by the Cabinet

In line with this mandate, the UAE National Space Strategy 2030 has been reviewed to ensure its alignment with the 17 Sustainable Development Goals (SDGs), the Long-Term Sustainability Guidelines, and the four pillars defined in the revised zero draft of the "Space2030" agenda, namely, space economy, space society, space accessibility, and space diplomacy. For each of the abovementioned

pillars, the following table contains implementation areas and actions in the UAE space sector.

Space2030 Agenda pillar	Implementation area	Actions in the UAE
<b>Space economy</b> <i>(Development of space-derived economic benefits)</i>	Increased involvement of international financial institutions	National Space Investment Promotion Plan and UAE NewSpace Innovation Program. Government investment institutions for various projects (Mubadala-Dubai Future Foundation, ADHC, etc.)
	Global partnership in space exploration and innovation	The Mohammad Bin Rashid Space Centre is currently working in cooperation with the UAE Space Agency and in the University of Colorado on manufacturing the Hope probe for Mars exploration
	Governmental support for the stimulation of start-ups to trigger increased private investments	There are incubators and accelerators for start-ups and entrepreneurs Special support funds for different projects (angel investors, venture capital funds, private equity funds) Public and private funding Several special economic zones (such as free economic zones)
<b>Space society</b> <i>(Evolution of society and societal benefits stemming from space-related activities)</i>	Better links to be created within the space society and in support of existing efforts (user needs)	The contribution of the space sector to other sectors such as transportation and agriculture sectors The contribution of the space sector to entities working in other sectors
	Capacity-building and awareness-raising efforts	Four research centers specific to space sciences and astronomy: Mohammed Bin Rashid Space Centre Sharjah Academy of Astronomy, Space sciences and Technology National Space Science and Technology Center Center for Space Science, NYU Abu Dhabi
	Gender balance in the space sector	National gender balance policy (under progress) New initiatives in the National Space Strategy: to stimulate and retain space sector personnel

(continued)

Space2030 Agenda pillar	Implementation area	Actions in the UAE
		while taking gender balance into consideration
	Inclusion of youth	The ratio of youth working in space sector is high Summer space camps for students
<b>Space accessibility</b> <i>(All communities using and benefiting from space technologies)</i>	Establishment of a capacity-building network	The UAE has developed national capacities and expertise in satellite manufacturing, assembly, integration, and testing Partnerships with international prestigious manufacturing companies to support the educational purposes Establish partnerships to build capacities (the UAE Ministry of Education, ICT fund) Host summer camp for students in collaboration with international institutes (e.g., Mission to Mars summer camp in Space School Hamilton College, Australia)
	Conducting of space exploration and innovation in an inclusive manner	The UAE Astronaut Programme
	Support and allow access to space for developing countries	Supporting other nations to establish space agencies and programs
<b>Space diplomacy</b> <i>(Building partnerships and strengthening international cooperation in space activities)</i>	Enhancing the safety, security, and sustainability of outer space activities	The UAE hosts space security-related events (Space Security Forum)
	Strengthening the global and regional presence	The UAE hosts several world conferences that include the participation of different groups of the space society, to share the developments and enhance cooperation regarding space activities United Nations High Level Forum on the role of space as an engine for sustainable development Space Congress 2019 Seminar of the United Nations Office for Outer Space Affairs and ICAO on aviation-space regulatory issues Space Risk Forum

(continued)







Space2030 Agenda pillar	Implementation area	Actions in the UAE
		Flight and Space Summit The membership of the UAE in the Committee of the Peaceful Uses of Outer Space, International Telecommunication Union, Space Exploration Coordination Group, Space Research Committee, International Astronautical Federation (IAF), and Space Navigation Coordination Group
	Participation in the process of establishing new elements of international outer space policy and governance	Aligning with: 17 Sustainable Development Goals and their 169 purposes for the SDGs Long-Term Sustainability Guidelines International space exploration roadmap for 2040 (ISECG Roadmap) Principles of space exploration
	Efforts to maintain space governance	The UAE is part of 10 out of the 15 major international conventions governing the use and exploration of outer space including: The 1967 treaty on principles governing the activities of states in the exploration and use of outer space, including the moon and other celestial bodies (Outer Space Treaty) The 1968 agreement on the rescue of astronauts, the return of astronauts, and the return of objects launched into outer space (Rescue Agreement) The 1972 convention on international liability for damage caused by space objects (Liability Convention) The 1975 convention on registration of objects launched into the outer space (Registration Convention) ITU CS/CV ITU RR and ITRs 1971 ITSO 1976 IMSO 1976 ARABSAT

(continued)



Space2030 Agenda pillar	Implementation area	Actions in the UAE
		<p>The UAE has developed the following national instruments:</p> <ul style="list-style-type: none"> <li>National Space Policy 2016</li> <li>National Space Strategy 2019</li> <li>National Space Law 2019</li> <li>Regulations and Procedures on Space Objects Registration 2018</li> <li>Regulation on Human Space Flight 2019</li> <li>Space Funding Policy 2017</li> <li>Space Investment Promotion Plan 2019</li> <li>Federal Decree for Application of Rescue Treaty 2017</li> <li>Regulation on Space Activity Authorization [2020]</li> <li>Regulation on Incident and Accident Investigation [2020]</li> <li>Regulation on Technical Audit of operators [2020]</li> <li>Guidelines for Space Data Policy [2020]</li> <li>Space Debris Mitigation Guidelines [2020]</li> </ul>
	Update existing instruments/ legal documents to reflect the new space era	Revised Regulations and Procedures on Space Objects Registration Revised Regulation on Human Space Flight
	Build constructive, knowledge-based partnerships	The UAE Space Agency cooperates with several international and regional space agencies: the USA, France, China, India, Japan, South Korea, Italy, Germany, Kazakhstan, Saudi Arabia, Egypt, Bahrain, and others
	International efforts to address space debris threats	Development of guidelines to mitigate space debris Propose incentives to comply with space debris mitigation guidelines and practices.
	Increased information exchange for effective space debris mitigation	New initiatives in the National Space Strategy Effective participation in the development of international space policies, decisions, laws, and regulations with focus on space debris mitigation

The UAE’s National Committee on SDGs conducted a mapping exercise between the UAE National Agenda, which includes a set of national indicators in different sectors, and the 2030 Agenda. At a thematic level, the 17 goals can be mapped to the pillars of the national agenda as shown in the following table:

#	National agenda	SDGs
1	Competitive knowledge economy	
2	Sustainable environment and infrastructure	
3	First-rate education system	
4	Cohesive society and preserved identity	
5	World-class healthcare	
6	Safe public and fair judiciary	

### The UAE Space Sector’s Contribution to the 17 SDGs

The UAE space sector is an active contributor toward achieving the sustainable development goals, where for each SDG, an indicator has been identified along with contribution description.

#### SDG 1: No Poverty

##### Indicator 1: Improved Communications as Driver for Growth

The United Arab Emirates owns and operates a number of communication satellites, namely, Thuraya Sats 1–3 for mobile satellite communications from 2000 to 2008; YahSAT Y1A for fixed communications and broadcasting, in addition to YahSAT Y1B for broadband services from 2011 to 2012; and YahSAT 3 in 2018 for broadband and broadcast with coverage of South America.

##### Indicator 2: Better Monitoring of Climate and Environment to Predict Crisis

An important breakthrough has been made in the area of modeling weather patterns. With the aid of supercomputer and data obtained by Himawari-8 satellite, Japanese scientists are able to measure the height of the top of clouds, which is of the essence for predicting wind and temperature. The program could have a strong impact in improving weather warnings, thus providing more time for evacuations (Japan forecasting breakthrough could improve weather warnings (2018)). Moreover,

Japan provided support in the creation and launching of Central America's first indigenously manufactured satellite used for monitoring carbon emissions in forests, as well as GhanaSat-1 cubesat, used for conducting research on monitoring illegal mining, water use, and deforestation (Successful deployment of five "BIRDS project" CubeSats from the "Kibo" 2017).

The UAE Space Agency and Mohammed Bin Rashid Space Centre are active members in the International Charter Space and Major Disasters. The International Charter is composed of space agencies and space system operators from around the world who work together to provide satellite imagery for disaster monitoring purposes. Types of disasters include cyclones, earthquakes, fires, floods, snow and ice, ocean waves, oil spills, volcanoes, and landslides.

In addition, the United Arab Emirates owns and operates a number of remote sensing satellites which supports the monitoring of environment, namely, the UAE remote sensing satellite DubaiSat-1, launched in 2009 with 4m resolution; the UAE remote sensing satellite DubaiSat-2, launched in 2013 with 1m resolution; and the UAE remote sensing satellite KhalifaSat, launched in 2018 with 0.6m resolution.

Furthermore, the UAE Space Agency is currently working along with academic institutes and research centers on a number of satellites and cubesats to support the monitoring of climate and environment such as MeznSat.

### **Indicator 3: Better Logistics Management**

Earth observation and remote sensing applications provide important information and data for policy-making and decision-making, particularly in the areas related to the protection of the environment and the management of disasters and crisis. Today the UAE owns and operates a number of Earth observation satellites where the latest is KhalifaSat which was launched in 2018 with 0.6m resolution. Nonetheless, there are ground station facilities for transmitting space-related data and providing value-added service. There are also other supporting services for rapid communication and modern information technologies and applications; transportation of all types, especially by air; availability of cargo and logistics services; customs services such as import and export; and travel and tourism.

### **Indicator 4: Offering Businesses and Jobs Opportunities**

Reference to the economic survey carried out by the UAE Space Agency and the Federal Competitiveness and Statistics Authority, the following results indicate that 22 entities working in the space sector have positively contributed to increasing business offerings and job opportunities (results for 2017) with a total workforce of 1513 employees, 37.4% of them UAE Nationals, 15% females, and 82.5% in specialized posts.

## **SDG 2: Zero Hunger**

### **Indicator 1: Optimized Agriculture**

The new 813 hyperspectral satellite is funded by the UAE Space Agency and will be developed by Arab engineers at the National Space Science and Technology Center at the United Arab Emirates University in Al Ain. The development of the satellite

will take 3 years and will have a lifespan of about 5 years. The planned launching year is 2023–2024. It will also have a polar orbit of 600km.

The data will be sent to a ground station in the UAE and receiving stations in some Arab countries for the benefit of a number of environmental authorities, municipalities, and institutions concerned with the agricultural sector and urban planning industry.

### **Indicator 2: Better Emergency and Aid Plans and Responses**

Space utilization plays a vital role in monitoring the weather, climate, and the environment; management of natural resource; crisis and disaster management; and rescue and humanitarian aid programs. Also, effective utilization of available space capacities in the UAE is in constant improvement; this is through enhancing coordination among local institutions that offer space services and applications, and the governmental entities concerned with natural disasters and national crisis management.

### **Indicator 3: Better Resources Management**

The UAE National Space Strategy 2030 includes an initiative that aims at enhancing national utilization of space services and capacities through integration between different space applications such as communications, Earth observation, remote sensing, and navigation. It seeks to enhance their integration with ground applications of communication, navigation, remote sensing, and others. It also aims to reach new applications and innovative solutions that support governmental, commercial, and research interests in different fields, such as transportation of all kinds, natural resources management, surveillance, energy, and the environment. Some of these initiatives are already reflected in several national projects such as DubaiSat, KhalifaSat, and DM SAT to support better management of resources including urban planning.

## **SDG 3: Good Health and Well-Being**

### **Indicator 1: E-Health, Including Telemedicine and Medical Teletraining and Learning**

There are many health portals that enable patients in the United Arab Emirates to view their health profiles, medical results, and book appointments online. An example is the smart patient portal system provided by the Ministry of Health and Prevention. A second example is e-Malaffi portal by Seha in Abu Dhabi. In addition to Salama Electronic Medical Record System which is under process by Dubai Health Authority (Healthcare providers 2019).

### **Indicator 2: Monitoring Public Health via EO Applications**

With the adoption of the 17 Sustainable Development Goals, and considering the important role of the UAE in supporting these objectives, as well as the role that space applications and services can play in achieving public health, efforts are being made toward enhancing the coordination between space service providers for Earth

observation, communications, and broadcasting, together with the concerned entities in the UAE in the fields of environment, climate change, natural resource management, health, human aid, and sustainable development in general. This is both to identify the needs of these entities and to identify the opportunities to utilize the space applications and services in addressing these needs.

## **SDG 4: Quality Education**

### **Indicator 1: Telelearning (Distance Learning)**

In October 2018, the United Arab Emirates government announced the official launch of Madrasa, a distance e-learning platform that provides 5000 free Arabic-translated videos in basic science, math, biology, chemistry, and physics. It also provides 11 million words on educational content to students from kindergarten to grade 12. Through satellite communications, more than 50 million Arab students from around the world are able to access to the online platform, hence establishing the foundations of self-learning, along with traditional educational institution, in addition to creating a new generation of qualified Arab researchers, scientists, and innovators that are capable of building knowledge-based societies and better future for their countries (eLearning, mLearning and distance learning 2019).

### **Indicator 2: Driver for STEM/ STEAM Education**

The space industry is closely linked to science, mathematics, engineering, technology, and design. Therefore, the development of specialized space competencies requires appropriate and attractive educational programs in these areas or the so-called “STEAM education.” The space industry is also an attractive area for students to participate in science, math, engineering, technology, and design activities as the industry is inspired by innovative ideas.

The UAE Space Agency supported and funded the creation of a remote sensing data clearing center at the UAE Space Agency. The goal is to establish a state-of-the-art remote sensing data clearing center at Zayed University to lead the development of Emirati scientists that will be in a position to utilize the data generated by Emirates Mars Mission as well as other sources of Earth observation data (multispectral and hyperspectral imaging) to solve environmental challenge.

## **SDG 5: Gender Equality**

### **Indicator 1: Women’s Active Role in Space Exploration, Science, Industry, Policy, and Diplomacy**

The UAE National Space Strategy 2030 includes an ongoing initiative focusing on stimulating and retaining space sector personnel while taking gender balance into account. The space professionals acquire high and unique skills and expertise that are compatible with space projects and various practical experiences. This initiative aims at preserving these competencies in the space sector especially the female competencies in the field as they constitute more than 40% of the workforce.

Reference to the economic survey carried out by the UAE Space Agency and the Federal Competitiveness and Statistics Authority (results for 2017), 47% of workforce in the top 12 UAE local entities in the space sector are females.

## **SDG 6: Clean Water and Sanitation**

### **Indicator 1: Water Management, Detection, Pollution Monitoring, and Distribution (Network Planning and Monitoring Logistics)**

The satellites images obtained through remote sensing have numerous applications about the water, for example, measuring water temperature. As such, the images that will be obtained from the hyperspectral satellite (813), which will be developed by engineers from the Arab region, will be used for that purpose among others.

## **SDG 8: Decent Work and Economic Growth**

### **Indicator 1: Space Services Enable Other Businesses Opportunities**

Recently, there has been an increasing number of emerging space programs in African and Latin American countries focusing on socioeconomic development and environmental monitoring. Examples of those programs include the launch of Algerian Alcomsat-1 satellite used for providing the Internet for neighboring countries and satellites launched by countries including Argentina, Costa Rica, and Ghana used for environmental and disaster monitoring. Moreover, four new countries (Australia, Egypt, Kenya, and New Zealand) have launched their national space agencies, thus accomplishing the first step of “space technology ladder.” Other countries making significant investment in their space program include Canada, South Korea, and Saudi Arabia (West and Stocker 2019).

## **SDG 9: Industry, Innovation, and Infrastructure**

### **Indicator 1: Private Sector Providing Various Space Services and Products**

The GeoTech Innovation Program is a collaborative project between the UAE Space Agency, and KryptoLabs is an innovation program that encompasses the selection of high potential entrepreneurs that can develop an application using satellite data in areas such as urban and rural land management, crisis and disaster management, and coastal border security.

Another program is the NewSpace program, which is a global space industry accelerator that aims to provide the support for entrepreneurs and start-ups in the space industry to align with the UAE Space Agency goals and objectives. Therefore, the program covers the value chain of entrepreneurship and innovation from ideation to growth to maximize the value-added for all beneficiaries and ensure high impact and returns.

### **Indicator 2: Innovative Launch Technologies**

The global space sector is witnessing significant developments in the capabilities and techniques in the field of launch vehicles in terms of reuse of vehicles or whether

these vehicles are very light or heavy. The small satellite revolution, the increase in interest by governments in space-related activities, the increase in demand for launch services, and the long waiting period in many cases have contributed to the remarkable commercial/private sector involvement in launch activities. Also, during the next phase, an increase in competition between the new and established institutions in the field is expected.

The Nation Space Strategy 2030 includes an initiative that aims to enhance the opportunity for the UAE to benefit from this boom in launch activities and to examine the best opportunities for investment whether in the development of launching vehicles, launching platforms, or operational capabilities in order to achieve economic return as well as guarantee and enhance access to space-related technologies.

### **Indicator 3: Innovative EO, Telecom, Navigation Applications**

The USA has been working on steadily improving the next-generation Global Positioning System, and the newly launched SV01 is expected to offer improved future connectivity worldwide for commercial and civilian use. Similarly, recently launched ESA's Galileo constellation of satellites is expected to deliver improved global coverage and more accurate pinpointing of Earth's locations. Chinese BeiDou satellites, which can offer accuracy comparable with GPS, were launched for providing communication and navigation services. Furthermore, as of 2017, India was in a process of completing its plans of launching its own GPS-type services for mobile users. In cooperation with GPS, the new Japanese positioning system, developed by joint efforts of JAXA and Mitsubishi Heavy Industries, is promising to reduce positioning errors to just a few inches (New orbiters for Europe's Galileo satnav system 2017) (India Plans to Roll Out National GPS Next Year 2017) (Kaneko and Perry 2017).

## **SDG 11: Sustainable Cities and Communities**

### **Indicator 1: EO Data for Safety, Disaster Management, Pollution and Climate Change Monitoring, Energy Management and Land Use Planning, and Monitoring Cultural Heritage**

The Italian-Argentine System of Satellites for Emergency Management is expected to use their SAOCOM 1A to create risk maps of plant diseases and flood recovery plans and detect humidity levels (Pacheco 2018). On top of that, there have been a significant number of the other recently launched satellites having the mutual goal of improving disaster planning and agriculture, as well as for controlling deforestation and climate changes. Some of them include South African EOSat1, Venezuelan VRSS-2, and Algerian Alcomsat-1.

Mohammed Bin Rashid Space Centre was established in 2015, encompassing previously existing Emirates Institution for Advanced Science and Technology (EIAST) as one of its affiliated institutions. So far, it has developed and launched three satellites, namely, DubaiSat-1, DubaiSat-2, and KhalifaSat, as well as Nayif-1, the first ever cubesat designed by Emirati engineers. Besides being the hub for

promoting space science and scientific research in the UAE and the whole region, it also provides significant support for other causes, including natural disasters management, rescue missions, and environmental monitoring (The UAE Space Sector 2018).

### **Indicator 2: Satcom for Telecom Services**

Al Yah Satellite Communications Company was established in 2007 and currently owns 5 fully operational satellites covering more than 160 countries. Its mission is to provide exceptional commercial, governmental, and military services, while at the same time focusing on further growth, empowerment of human capital, and quality enhancement. Thuraya Telecommunications Company was established in 1997 with the goal of providing global mobile communication services. It covers two third of the Earth, and its most recent achievement is the production of the world's first Android based satellite and GSM phone (Thuraya 2019).

## **SDG 12: Responsible Consumption and Production**

### **Indicator 1: Sat/Nav for Logistics Management in Production**

The UAE has support services for the space industry and its activities such as communications, transportation, shipping, logistics, customs clearance, import and export, and travel and tourism.

Organizations operating in the UAE space sector, including research and development centers, rely on the availability of services that support their work to carry out their activities and space projects. Such services include high-speed telecommunication services, modern information technology and transportation, aviation, logistics, customs services, import and export, and travel and tourism services. As for start-ups, it is important to provide incubation facilities and accelerators for innovation and entrepreneurship. The quality and low cost of these services are attractive elements for these institutions. For that, the UAE National Space Strategy 2030 includes an initiative focusing on evaluating and providing recommendations on current and future needs for infrastructure, facilities, and other logistical services supporting institutions and space activities.

## **SDG 13: Climate Action**

### **Indicator 1: Earth Observation Data Key for Climate Change, Pollution Monitoring, and Mitigation Strategies**

The research in predicting harmful space weather has been active in the recent time as well. Agencies such as NOAA, USAF, and ESA are actively working on studying space weather events. NOAA and USAF jointly run the center for potential disturbances of people and equipment in space environment, while ESA operates a warning network for monitoring solar storms. The US space weather program currently has a technology for predicting and warning about severe solar storm half an hour before they happen. The World Meteorological Organization (WMO) is in the process of integrating space weather effort into its integral part of its work



and facilitation of coordination with external players, which should result in improved space weather service capabilities (Sutherland 2015).

## **SDG 14: Life Below Water**

### **Indicator 1: Space Science and Technologies for Efficient Use of Water Resources Including Preservation**

Programs such as Copernicus, jointly run by ESA and European Commission and Italy's COSMO-SkyMed, utilize the space-based capabilities for observing Earth's surface, ocean levels, and climate (Zosimovych and Chen 2018). The European Global Navigation Satellite Systems Agency holds a responsibility for the operation of Galileo satellites used for global navigation. In cooperation with Japan, Europe is leading BepiColombo mission with the aim of examining Mercury's magnetic fields and polar regions for the presence of water (DEPICOLOMBO n.d.).

## **SDG 15: Life on Land**

### **Indicator 1: EO Data for Biodiversity Monitoring, Pollution Monitoring, and Land Use Management and for Compliance and Policing**

The UAE Space Agency is working on a land cover and land use mapping for the whole UAE in collaboration with a number of national stakeholders. The goal of this project is to develop a land cover and land use map product for the entire UAE using the high resolution of satellite images. This will lead to the development of local capabilities in the field and positive contribution toward updating the developed maps.

## **SDG 17: Partnerships for the Goals**

### **Indicator 1: PPP at Local Levels (Public + Industry + R&D + Academia)**

There are a number of partnership projects between local UAE entities. First project is between the UAE Space Agency and Khalifa University in manufacturing a scientific and educational satellite for studying the Earth's atmosphere (MiznSat) where the launching year is 2020. The second project is between the UAE Space Agency and UAE University in manufacturing a scientific and technology testing satellite focusing on Global Navigation Satellite System (GNSS) to be launched in 2020. Third is a project between the UAE Space Agency and Khalifa University and the National Authority for space science in Bahrain in manufacturing a scientific and educational satellite to be launched in 2020 as well. Fourth is a project between YahSat and Khalifa University in manufacturing MySat, an educational satellite to be launched in 2021. Fifth is a project between Mohammed Bin Rashid Space Centre and Dubai Municipality in manufacturing DMSat, an educational and services satellite to be launched in 2019. Sixth is a project between the UAE Space Agency and the National Space Science and Technology Center in manufacturing an educational and services hyperspectral satellite. Planned launching year is 2023–2024.

### **Indicator 2: Space and non-Space Actors**

The UAE generally enjoys strong cooperation and partnerships at the regional and international levels, especially in political, economic, and commercial terms, hence supporting its space-related cooperation and companies.

Also, reference to the economic survey carried out by the UAESA and FCSA (results for 2017), the number of sectors benefiting from space services and activities is 17. Examples of benefiting sectors include telecommunications, education, energy, tourism and leisure, high-tech industries, and agriculture. It is worth noting that the number of contracted entities benefiting from space services and activities is 709, where 268 are within the UAE and 441 are outside UAE.

### **Indicator 3: International Collaboration and Partnerships**

The UAE Space Agency cooperates actively with several international and regional space agencies such as the USA, France, China, India, Japan, South Korea, Italy, Germany, Kazakhstan, Bahrain, and others. The UAE have also signed more than 25 MoUs/agreements with international space partners for carrying out projects feeding toward the national space program, and its initiatives, and is a member of the Committee of the Peaceful Uses of Outer Space, International Telecommunication Union, Space Exploration Coordination Group, Space Research Committee, International Astronautical Federation (IAF), and the Space Navigation Coordination Group

The UAE had the privilege to host a number of prominent satellite events such as the United Nations High Level Forum on the role of space as an engine for sustainable development back in 2015, the seminar of the United Nations Office for Outer Space Affairs and ICAO on aviation and space regulatory issues, the Space Risk Forum, and the Flight and Space Summit, including others.

---

## **The UAE Space Policy Contribution to the LTS Guidelines**

The long-term sustainability of outer space activities is defined as the ability to maintain the conduct of space activities indefinitely into the future in a manner that realized the objectives of equitable access to the benefits of the exploration and use of outer space for peaceful purposes, in order to meet the needs of the present generations while preserving the outer space environment for future generations (Guidelines for the Long-term Sustainability of Outer Space Activities 2018). As such, in June 2016, the committee on the peaceful uses of outer space agreed to a first set of guidelines for the long-term sustainability of outer space activities addressing policy, regulatory, operational, safety, scientific, technical, international cooperation, and capacity-building aspects. In June 2019, a set of nine additional guidelines for long-term sustainability of outer space activities of the Committee of the Peaceful Uses of Outer Space were adopted (Long-term Sustainability of Outer Space Activities 2019).

UNCOPUOS encourages states and international intergovernmental organizations to voluntarily take measures to ensure that the guidelines are implemented to

the greatest extent. Accordingly, the United Arab Emirates policy efforts in achieving the guidelines are highlighted below.

## **LTS Guideline A: Policy and Regulatory Framework for Space Activities**

### **Guideline A.1: Adopt, Revise, and Amend, as Necessary, National Regulatory Frameworks for Outer Space Activities**

The open nature of space requires a robust international legal framework to ensure the harmonization of domestic space laws among nations with space programs. The UAE Space Agency works to represent and reflect the UAE's interests to the international community through active participation and contribution to key international organizations and forums related to outer space. Simultaneously, the UAE will continue to respect international laws and norms when developing and maintaining domestic legislation and regulations.

The UAE is currently a signatory to four out of the five main international space treaties, namely:

- Outer Space Treaty 1967: Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies
- Rescue Agreement 1968: Agreement on the Rescue of Astronauts, the Return of Astronauts and Return of Objects Launched into Outer Space
- Liability Convention 1972: Convention on International Liability for Damage Caused by Space Objects
- Registration Convention 1975: Convention on Registration of Objects Launched into Outer Space

The UAE has issued more than eight national space policy and regulatory documents, including the National Space Policy, the National Space Strategy 2030, the Federal Law on Regulating the Space Activities, and several others.

### **Guideline A.2: Consider a Number of Elements when Developing, Revising, or Amending, as Necessary, National Regulatory Frameworks for Outer Space Activities**

The UAE Space Agency is responsible for drafting the legal framework for the UAE's space sector. The National Space Law will be the first of its kind in the region, providing a legislative and legal framework for the space sector that is in line with the UAE federal policies and international laws and regulations.

The National Space Law, which was approved in December 2019, covers the organization and objectives of space projects undertaken by the country, including peaceful space exploration and the safe use of space technologies. It also addresses new and complex concepts, such as the right to own resources found in space, organizing manned space travel, and other commercial activities, such as asteroid mining.

The following considerations were taken into account when drafting the UAE National Space Law:

- The provisions of the General Assembly Resolution 68/74, on recommendations on national legislation relevant to peaceful exploration and use of outer space
- The Space Debris Mitigation Guidelines of UNCOUPOS.
- Potential risks associated to implementing space activities
- Promoting regulations and policies that support sustainability of space and the Earth
- Guidance contained in the Safety Framework for Nuclear Power Source Applications in Outer Space
- Potential benefits of using existing international technical standards, including those published by the International Organization for Standardization (ISO), the Consultative Committee for Space Data Systems, and national standardization bodies
- Legal capacities of imposed regulations
- Advisory input from affected national entities during the development process
- Existing relevant legislations

### **Guideline A.3: Supervise National Space Activities**

The UAE Space Agency is a federal agency that was created under Federal Law by Decree No. 1 of 2014. The agency has the mandate to oversee the space sector activities and develop and roll out national space policies and legislations.

The UAE Space Agency works to represent and reflect the United Arab Emirate's interests to the international community through active participation and contribution to key international organizations and forums related to outer space. Simultaneously, the UAE continues to adhere to and respect international laws and norms when developing and maintaining domestic legislation and regulations.

### **Guideline A.4: Ensure the Equitable, Rational, and Efficient Use of the Radio Frequency Spectrum and the Various Orbital Regions Used by Satellites**

The UAE has been able to develop national competencies specialized in the areas of spectrum management in general and the management of space frequencies and orbits, in particular. That is done through the programs and initiatives of the National Space Strategy 2030, which includes program 6.3 that focuses on effective management and coordination of the interests of the space sector regarding the radio spectrum and orbital positions. The program includes a number of initiatives such as the identification of frequency bands and orbital positions of priority to the UAE's space-related activities and the development of standards, procedures, and capacities to increase the efficiency of spectrum and orbital use as well as situational awareness.

### **Guideline A.5: Enhance the Practice of Registering Space Objects**

In order to maintain an up-to-date record of UAE space objects and to fulfill the obligations under the 1976 Registration Convention, the UAE Space Agency is

responsible for the development and maintenance of the National Register of Space Objects and also responsible for notifying, via the Ministry of Foreign Affairs, the United Nation Office of Outer Space Affairs (UNOOSA) for the registration and updating the statuses of the UAE space objects in the International Space Object Register.

## **LTS Guideline B: Safety of Space Operations**

### **Guideline B.1: Provide Updated Contact Information and Share Information on Space Objects and Orbital Events**

In 2018, the UAE issued the Space Objects Registration Regulation, and in 2019, the UAE Space Agency ensured the 100% registration of the UAE Space Objects at the UNOOSA Register of Space Objects.

### **Guideline B.2: Improve Accuracy of Orbital Data on Space Objects and Enhance the Practice and Utility of Sharing Orbital Information on Space Objects**

The UAE, when sharing orbital information on space objects and operators, ensures using commonly used method that is compliant with international standards, and hence facilitating wider distribution and awareness of current and predicted location of space objects.

As such, and in regard to space debris object WT1190F, an airborne observing campaign was organized to practice the rapid response to announced small asteroid impacts by the UAE Space Agency and in collaboration with International Astronomical Center, NASA, and ESA. Also, in 2016, the UAE Space Agency established the Science, Technology and Innovation Roadmap where space debris and meteorites were flagged as an area of interest.

### **Guideline B.3: Promote the Collection, Sharing, and Dissemination of Space Debris Monitoring Information**

Due to the ever-increasing volume of space activity, and resulting space debris, nearby outer space already requires a special treatment and protection from the entire humankind. Consequently, the UAE Space Agency completed the development of guidelines to mitigate space debris. Also, the National Space Strategy 2030 includes an initiative focusing on effective participation in the development of international space policies, decisions, laws, and regulations with focus on space debris mitigation.

### **Guideline B.4: Perform Conjunction Assessment During All Orbital Phases of Controlled Flight**

In compliance with Article VI of the 1967 Outer Space Treaty, the UAE ensures that conjunction assessment is conducted by all space craft operators during all orbital phases of controlled flight for their current and planned spacecraft trajectories.

**Guideline B.7: Develop Space Weather Models and Tools and Collect Established Practices on the Mitigation of Space Weather Effects**

The National Space Strategy 2030 confirms the United Arab Emirates commitment for the next decade toward enhancing space R&D activities, capacities, and efforts, namely, in launching research projects in high national priority fields with a focus on conducting research on best practices and technologies to manage space risks and space traffic and to track and reduce the effects of space debris and space weather.

**Guideline B.9: Take Measures to Address Risks Associated with the Uncontrolled Reentry of Space Objects**

The National Space Strategy 2030 confirms the United Arab Emirates commitment in ensuring a supporting legislative framework and infrastructure to match the future developments in the sector, namely, in establishing an investigation mechanism for space-related accidents and incidents during their launch or reentry. The mechanisms investigate these cases efficiently and effectively to identify their causes, the lessons learned from such incidents, and the opportunities for improvement.

**Guideline B.10: Observe Measures of Precaution when Using Sources of Laser Beams Passing Through the Outer Space**

Through the National Space Strategy 2030, program 6.3 on effective management and coordination of the interests of the space sector regarding the radio spectrum and orbital positions includes an initiative focusing on the development of standards, procedures, and capacities to increase the efficiency of spectrum and orbital use as well as situational awareness. As such, the UAE working team will consider issues related to the management of space frequencies, such as the use of laser and frequency management on the surfaces of other celestial bodies.

**LTS Guideline C: International Cooperation, Capacity-Building, and Awareness****Guideline C.1: Promote and Facilitate International Cooperation in Support of the Long-Term Sustainability of Outer Space Activities**

In March 2019, the Arab Space Cooperation Group was announced, setting a huge milestone toward sharing of experiences related to long-term sustainability of outer space activities, expertise, and information exchange. The prime objective of the group is to exchange knowledge, boosting the Arab space industry and working on joint projects. The group's first project "813" will be a remote sensing/Earth observation satellite built by Arab space specialists from all countries in the group. It will aim to tackle climate and environmental issues in the Arab world and other parts of the globe.

The National Space Investment Promotion Plan, announced in 2019, provides a high-level approach to facilitate more investments in the United Arab Emirates space industry and contribute toward the alignment of the government goals stated in the UAE Vision 2021, the UAE 2071, and the UAE Plan on the fourth industrial

revolution, in particular, to diversify and ensure sustainability of the UAE economy, to promote highly productive knowledge-based economy, to provide incentives for R&D and innovation, and encourage entrepreneurship, and SMEs role and opportunities in the private sector. Additionally, The UAE NewSpace Innovation Program is a joint initiative by the UAE Space Agency and Krypto Labs to accelerate the growth of four tech businesses in the field of NewSpace, which refers to the rise of the private spaceflight industry that aims to make space more accessible, affordable, and commercial, for scientists and the general public. The program falls under the National Space Investment Promotion Plan which aims to heighten the role of the space industry in contributing to the economy of the UAE, while encouraging a culture of interest in the space sector, in efforts to establish a knowledge-based competitive national economy built on innovation and the latest technologies.

Moreover, and in accordance with the 2018 space economy survey conducted by the UAE Space Agency, the total number of entities working in the United Arab Emirates space economy is 52, with more than 3100 people working in the UAE space economy; 40% of them are below 35 years. To date, in more than 17 sectors, 1232 contracted entities are benefiting from the UAE space services and applications, in particular more than 750 from inside the state, whereas 480 and from international entities. Nevertheless, the main and most benefiting sectors are telecommunications, education, data analytics and LBS, science and R&D, tourism, transportation, and urban planning.

### **Guideline C.2: Share Experience Related to the Long-Term Sustainability of Outer Space Activities and Develop New Procedures, as Appropriate, for Information Exchange**

In alignment with the United Arab Emirates efforts to promote international cooperation to enable all countries through the exchange of expertise in developing national space policies and regulations in support of these guidelines, a number of knowledge transfer workshops were conducted during 2019, namely, with space agencies in Egypt, Kingdom of Saudi Arabia, and Republic of Azerbaijan.

The National Space Strategy 2030 confirms the United Arab Emirates commitment for the next decade toward achieving relevant strategic objectives, namely, in creating space culture and expertise with 3 supporting programs and 11 initiatives, as well as in promoting effective local and global partnerships and investments in the space industry by outlining 3 programs and 15 initiatives.

To date, the UAE Space Agency has signed more than 30 agreements and cooperation MOUs to promote and facilitate international cooperation with space agencies and organizations in support of the long-term sustainability of outer space activities. These agreements create the basis for further collaborative activities between countries in mutually agreed projects, and priority areas.

### **Guideline C.3: Promote and Support Capacity-Building**

The Hope Mars Mission is a planned space exploration probe mission to Mars which is funded by the UAE Space Agency and is built by the Mohammed Bin Rashid

Space Centre, the University of Colorado, and Arizona State University. The mission is set for launch from Japan in the summer of 2020 with the aim of enriching the capabilities of Emirati engineers and increasing human knowledge about the Martian atmosphere. This is An example of a collaborative scientific project with foreign research institutions, in contribution toward a knowledge-based economy.

The UAE Space Agency undertakes efforts to support capacity-building initiatives and promote new forms of national, regional, and international cooperation to improve space-related expertise and knowledge. The UAE government sponsored more than 100 distinguish students to study space fields in and outside the UAE, conducted in 2019 alone more than 17 space-specialized trainings and education camps and sessions, launched rocket assembly competition with 167 participants,

sponsored qualified students to join the NASA International Internship Program (NASA I<sup>2</sup>), which provides an environment for US and non-US university undergraduate-level or graduate-level students to work collaboratively on NASA-relevant research with a NASA mentor, and also conducted a number of awareness and training workshops under the future scientists program in collaboration with Airbus, and provided sponsorship for several students to attend the Space Generation Congress and the science workshops.

#### **Guideline C.4: Raise Awareness of Space Activities**

The UAE is committed to increasing the effectiveness and diversity of its awareness-raising activities for the space industry in the state as well as for the space industry in general. It is ensured that all awareness activities target different segments of the public and highlight the achievements in this scientific and inspiring field.

It also seeks to coordinate efforts to achieve efficiency, diversity, and integration of awareness-raising programs. As such, the UAE hosted several world conferences that include the participation of different groups of the space society, to share the developments and enhance cooperation regarding space activities. To name few, in 2019, the UAE was the first Arab country to host the international conference Young Professionals in Space (YPS) which provided a valuable opportunity for Arab youth to connect with experts and scientist and share insights on future contributions to solutions for humanity.

Moreover, strategic global space industry leaders and more than 600 key space agencies, commercial space organizations, academic institutions, and users of space services were brought together on the sidelines of the Global Space Congress in 2019, an event hosted by the UAE Space Agency offering a unique experience on the biggest opportunities in the space sector by providing exposure to worlds most vibrant and energetic space programs.

Also, in 2019, the Humans in Space Symposium was organized by the Mohamed bin Rashid Space Centre where experts from around the world gathered to discuss topics such as the challenges in of future space flights, biology and biotechnology in space, and Mars exploration. The symposium offered a multidisciplinary discussions involving the exchange of research results and ideas in the field of space science, as well as sharing of UAE's recent experience and expertise in the area of human spaceflight.



In October 2020, the UAE will be the first country in the entire region to host one of the most premiere space events, the 71st International Astronautical Congress. The Mohammed bin Rashid Space Centre is committed toward making this event a sounding success with the attendance of world decision-makers in an iconic meeting of minds, working toward the advancement of space science and technology, and ultimately the betterment of all humankind.

The UAE will continue to raise awareness of space activities through initiative implementation of strategic objective 4 in the National Space Strategy 2030, namely, creating a high level of national space culture and expertise. One example is the development of an informative program to spread knowledge about the national achievements in space and about the space sector in general. This is achieved through the development of a diverse and renewable informative program to spread general knowledge about space among the different social groups, as well as the launch of an international campaign to promote awareness about the national space sector.

## **LTS Guideline D: Scientific and Technical Research and Development**

### **Guideline D.1: Promote and Support Research into and the Development of Ways to Support Sustainable Exploration and Use of Outer Space**

The United Arab Emirates is continuously working on the development and sustainability of ambitious activities in space sciences and exploration. It reconfirms its commitment in increasing the state contribution to the space science community.

The Emirates Space Innovation Group (ESIG) is a UAE Space Agency project designed to increase opportunities for national space activities and strengthen engagement throughout the local space sector with agency-funded missions and projects. ESIG aims to advance science, technology, and innovation on a local level and coordinate projects being implemented by the various space sector actors and stakeholders. ESIG is made up of government agencies, companies, universities, and research centers throughout the state. The group meets on a quarterly basis to discuss the latest updates related to a number of space projects and activities taking place nationwide. Meetings also cover ongoing projects and future funding of missions and research.

In 2017, The United Arab Emirates government announced its ambitious inspiring scientific space exploration project that aims at building the first complete inhabitable human settlement on the surface of Mars in 2117, with the objective of planting the seed today in the hope for future generations to reap the benefits, driven by its passion to learn to unveil a new knowledge. In order to achieve this ambitious program with excellence, a practical plan is being developed in partnership with national capacities and expertise, regional and international partnerships, as well as international scientists and experts opinions on the subject.

In 2018 alone, a total of 64 scientific research papers were published, and up to 24 space inventions were registered. To further support the sector, the National

Space Strategy 2030 includes a strategic goal with 3 programs and 11 initiatives, namely, launching inspiring space scientific and exploration programs.

In 25 September 2019, the UAE celebrated the launch of its first Emirati astronaut, as part of the UAE Astronaut Program, to the ISS where he conducted more than 16 scientific experiments. In July 2020, the UAE intends to launch the Hope Probe to Mars, the first deep space exploration mission in the Arab and Islamic world. The Mission aims to study the atmosphere of the red planet.

As part of the Mars 2117 Program, launched during the fifth World Government Summit, the Mars Science City project falls within the United Arab Emirates' objectives to contribute to the global scientific race to take people to Mars. This project will include advanced laboratories that simulate the red planet's terrain and harsh environment through advanced 3D printing technology and heat and radiation insulation. It seeks to attract the best scientific minds from around the world in a collaborative contribution in the state to human development and the improvement of life. It also seeks to address global challenges such as food, water, and energy security on Earth.

### **Guideline D.2: Investigate and Consider New Measures to Manage the Space Debris Population in the Long Term**

The UAE is committed toward investigating new measures to manage the ever-increasing accumulation of space debris in outer space. As such, the UAE Space Agency has completed two detailed studies on the topic where a comparative analysis of technical and legal considerations was conducted, resulting in reports containing a set of recommendations and worldwide best practices. In addition, assessing the development of new space-related activities technologies and applications, the necessary authorization system for these activities is being developed. Such procedures would also take into account measures necessary to maintain safety and stability in the space environment which will include the development of guidelines to mitigate space debris.

---

## **Conclusions**

The present chapter has outlined the UAE's efforts and contributions in achieving space security, the sustainable development goals of Agenda 2030, and the long-term sustainability of outer space.

Space utilization and discoveries have been able to enrich the human knowledge of the universe and contribute to improving the daily lives of humans. The leadership of the UAE has realized the increasing importance of the space sector and has supported its continuous growth on a regional and global level, justifying its investment in the sector since the early 1990s. Today the UAE is proud to have a strong and diverse space sector, which over the past three decades has managed to develop capacities and expertise qualifying it to compete globally and to move on to a new phase in its national program for space.

The National Space Strategy 2030 aims at supporting the achievement of this national vision by the space industry with its different sciences, technologies, applications, and services. It also translates the space policy issued in 2016 into a group of programs and initiatives that the space sector in the state will work on executing during the coming decade, with the purpose of reaching the national ambitions drawn by the space policy.

The National Space Law, which was approved in December 2019, covers the organization and objectives of space projects undertaken by the country, including peaceful space exploration and the safe use of space technologies. It also addresses new and complex concepts, such as the right to own resources found in space, organizing manned space travel, and other commercial activities, such as asteroid mining.

Nevertheless, The UAE will continue to work on the development of regulatory environment attractive to the different space activities. Such would be transparent and futuristic, one that balances the safety, security, and environmental needs on one side and the economic, commercial, and innovative needs on the other. It will also enhance the efforts internationally in decision-making and the alignment between local and global regulations. It will continue to work alongside its national and international partners in implementing the necessary measures in achieving space sustainability. As a responsible national organization, the UAE Space Agency is committed to foster and dedicate its local competences and technology for the betterment of humankind.

---

## References

- Building UAE Space Capabilities (2017) UAE Space Agency. Retrieved from [http://www.unoosa.org/documents/pdf/hlf/1st\\_hlf\\_Dubai/Presentations/51.pdf?fbclid=IwAR2DNXEd\\_kqhrehL1sGi\\_q1XzARfKR36ud44WzVAUrz4vhpM814bhIW9i8](http://www.unoosa.org/documents/pdf/hlf/1st_hlf_Dubai/Presentations/51.pdf?fbclid=IwAR2DNXEd_kqhrehL1sGi_q1XzARfKR36ud44WzVAUrz4vhpM814bhIW9i8)
- DEPICOLOMBO (n.d.). Retrieved from <https://sci.esa.int/web/bepicolombo>
- eLearning, mLearning and distance learning (2019, September 08) Retrieved from government.ae: <https://www.government.ae/en/information-and-services/education/elearning-mlearning-and-distant-learning>
- Guidelines for the Long-term Sustainability of Outer Space Activities (2018, June 27) Retrieved from United Nations Office for Outer Space Affairs: [https://www.unoosa.org/res/oosadoc/data/documents/2018/aac\\_1052018crp/aac\\_1052018crp\\_20\\_0\\_html/AC105\\_2018\\_CRP20E.pdf](https://www.unoosa.org/res/oosadoc/data/documents/2018/aac_1052018crp/aac_1052018crp_20_0_html/AC105_2018_CRP20E.pdf)
- Healthcare providers (2019, December 12) Retrieved from government.ae: <https://government.ae/en/information-and-services/health-and-fitness/healthcare-providers>
- Hui J (2018) The Spatial Information Corridor Contributes to UNISPACE+50. Retrieved from <http://www.unoosa.org/documents/pdf/copuos/stsc/2018/tech-08E.pdf>
- India Plans to Roll Out National GPS Next Year (2017, July 07) Retrieved from GPS Daily: [http://www.gpsdaily.com/reports/India\\_Plans\\_to\\_Roll\\_Out\\_National\\_GPS\\_Next\\_Year\\_999.html](http://www.gpsdaily.com/reports/India_Plans_to_Roll_Out_National_GPS_Next_Year_999.html)
- Japan forecasting breakthrough could improve weather warnings (2018, January 17) Retrieved from Space Daily: [http://www.spacedaily.com/reports/Japan\\_forecasting\\_breakthrough\\_could\\_improve\\_weather\\_warnings\\_999.html](http://www.spacedaily.com/reports/Japan_forecasting_breakthrough_could_improve_weather_warnings_999.html)
- Kaneko K, Perry M (2017, June 01) Japan launches its version of GPS satellite to improve location positioning. Retrieved from Reuters: <https://www.reuters.com/article/us-japan-satellite/japan-launches-its-versionof-gps-satellite-to-improve-location-positioning-idUSKBN18S3WG>

- Long-term Sustainability of Outer Space Activities (2019) Retrieved from United Nations Office for Outer Space Affairs: <https://www.unoosa.org/oosa/en/ourwork/topics/long-term-sustainability-of-outer-space-activities.html>
- MBRSC (2019) Retrieved from KhalifaSat: <https://www.mbrsc.ae/satellite-programme/khalifasat>
- Moltz JC (2002) Future security in space: commercial, military, and arms control trade-offs. University of Southampton/Center for Nonproliferation Studies, Monterey. Retrieved from <http://www.nonproliferation.org/wp-content/uploads/2016/09/op10.pdf>
- New orbiters for Europe's Galileo satnav system (2017, June 22) Retrieved from GPS Daily: [http://www.gpsdaily.com/reports/New\\_orbiters\\_for\\_Europes\\_Galileo\\_satnav\\_system\\_999.html](http://www.gpsdaily.com/reports/New_orbiters_for_Europes_Galileo_satnav_system_999.html)
- Outer Space and Security (2014) In: J. M. Defense, Defense of Japan. pp 105–108. Retrieved from [https://www.mod.go.jp/e/publ/w\\_paper/pdf/2014/DOJ2014\\_1-2-4\\_web\\_1031.pdf?fbclid=IwAR21XzkwrU2ZKjknxlfH6ox9NnaW8VK8qgS3WCfcWz2s0msqBtmgwZDBgig](https://www.mod.go.jp/e/publ/w_paper/pdf/2014/DOJ2014_1-2-4_web_1031.pdf?fbclid=IwAR21XzkwrU2ZKjknxlfH6ox9NnaW8VK8qgS3WCfcWz2s0msqBtmgwZDBgig)
- Outer Space Treaty of 1967 (n.d.). Retrieved from <https://history.nasa.gov/1967treaty.html>
- Pacheco C (2018, January 04) SpaceX is launching an Argentine satellite in 2018, and here's what it'll do. Retrieved from <https://www.thebubble.com/spacex-is-launching-an-argentine-satellite-in-2018-and-heres-what-itll-do>
- Space Security Index (2019) Canada: Spacesecurityindex.org. Retrieved from <http://spacesecurityindex.org/wp-content/uploads/2019/10/SSI2019ExecutiveSummaryCompressed.pdf>
- Successful deployment of five "BIRDS project" CubeSats from the "Kibo" (2017, July 07) Retrieved from Japan Aerospace Exploration Agency: [http://iss.jaxa.jp/en/kiboexp/news/170707\\_cubesat\\_birds.html](http://iss.jaxa.jp/en/kiboexp/news/170707_cubesat_birds.html)
- Sutherland S (2015, November 6) New plans emerge to deal with looming risks of space weather. Retrieved from The Weather Network: [www.theweathernetwork.com/news/articles/white-houseesa-plans-promise-better-response-to-space-weather-risks/59482](http://www.theweathernetwork.com/news/articles/white-houseesa-plans-promise-better-response-to-space-weather-risks/59482)
- The Economic Times (2017, October) Retrieved from UAE Space Agency signs MoU with Luxembourg: <https://economictimes.indiatimes.com/news/science/uae-space-agency-signs-mou-with-luxembourg/articleshow/61024984.cms>
- The UAE Space Sector (2018, April). Retrieved from [https://www.sasic.sa.gov.au/docs/default-source/5th-sa-space-forum-presentations/1015%2D%2D-naser-al-hammadi-and-abir-khater.pdf?fbclid=IwAR15esz2d2AkXEEEDLYyK00u8gGzwfEjFavDjVx2WL\\_OYAH8FtYfXkSROtZY](https://www.sasic.sa.gov.au/docs/default-source/5th-sa-space-forum-presentations/1015%2D%2D-naser-al-hammadi-and-abir-khater.pdf?fbclid=IwAR15esz2d2AkXEEEDLYyK00u8gGzwfEjFavDjVx2WL_OYAH8FtYfXkSROtZY)
- Thuraya (2019). Retrieved from <https://www.thuraya.com/x5-touch>
- United Nations/United Arab Emirates High Level Forum: Space as a driver for socio-economic sustainable development (2017). Retrieved from <http://www.unoosa.org/documents/pdf/hlf/HLF2017/AnnouncementHLF2017.pdf>
- West J, Stocker W (2019, October) Space Security Index. Retrieved from <http://spacesecurityindex.org/wp-content/uploads/2019/10/SSI2019ExecutiveSummaryCompressed.pdf>
- Zosimovych N, Chen Z (2018, September) CubeSat Design and Manufacturing Technique Analysis. Retrieved from IOSR Journal of Engineering: [http://www.iosrjen.org/Papers/vol8\\_issue9/Version-5/A0809050106.pdf](http://www.iosrjen.org/Papers/vol8_issue9/Version-5/A0809050106.pdf)



Olavo de O. Bittencourt Neto and Daniel Freire e Almeida

## Contents

Introduction .....	654
Space Security and Emerging Space Faring Nations .....	656
Brazilian Space Policy: An Overview .....	656
Domestic Regulatory Instruments .....	659
Brazilian Space Situational Awareness Initiatives .....	662
Prevention of Arms Race in Outer Space: Brazilian Perspectives .....	664
Conclusions .....	665
References .....	666

## Abstract

The present chapter provides updated information regarding Brazilian space law, policy, and initiatives related to space security, considering applicable perspectives. The secure and sustainable access to, and use of, outer space is obviously important to the international community in general, but of particular relevance to emerging space faring nations, which tend to experience overreliance in relation to a small selection of space assets. Appraising the Brazilian perspective on space security contributes to a better understanding of the challenges faced by emerging space faring nations on that regard, acknowledging their particularities as well as possible synergies. To that end, this chapter, after a brief introduction, clarifies the importance of space security for emerging space faring nations. Then, an overview of related Brazilian space policy is presented, followed by an examination of space safety related regulatory instruments. Brazilian position on the prevention of an arms race in outer space is appraised, considering current international debates. Finally, reference is made to local space situational awareness initiatives, and future prospects are considered.

O. d. O. Bittencourt Neto (✉) · D. Freire e Almeida  
Catholic University of Santos, Santos, Brazil  
e-mail: [olavo.bittencourt@unisantos.br](mailto:olavo.bittencourt@unisantos.br); [danielfreire@unisantos.br](mailto:danielfreire@unisantos.br); [da616@georgetown.edu](mailto:da616@georgetown.edu)

---

**Keywords**

Space security · Space situational awareness · Space law and policy · Brazil

---

**Introduction**

Nowadays, space security emerges as a global concern, not only to governments but also to the private sector as well, decurrent from increasing worldwide dependability over a wide range of space activities, not only to governments, leading to the support of different but interrelated initiatives toward long-term sustainability of outer space (Casella 2009). Ranging from domestic legislation to industrial guidelines, those frameworks focus on major threats to space-based assets and systems, most specifically relating to condition and knowledge of the space environment, access to and use of outer space by different actors and security of space systems themselves.

One may affirm that space activities in general, whether encompassing space vehicles, artificial satellites, launching centers, collection or remittance of data, and their related applications, would clearly benefit from governance initiatives designed to address relevant vulnerabilities. Emerging space-faring nations are no stranger to those complications, enhanced by insufficient redundancy, as far as space objects are concerned; therefore, appropriate measures have increasingly been under consideration, in different regulatory levels, deserving to be properly accessed in view of possible synergies.

Domestic guidelines on space security initiatives, as verified in certain emerging space-faring nations, represent relevant initiatives fully supported by International Law. In fact, the fundamental framework provided by applicable multilateral treaties is in a straight line with the prerogative of States in relation to their rights of self-defense and of autonomous regulation of national space activities.

A brief assessment of certain international instruments is justified for our study, starting from the United Nations Charter, of 1945. Accordingly, the first purpose of this important international organization is solemnly stated as being “*to maintain international peace and security, and to that end: to take effective collective measures for the prevention and removal of threats to the peace, and for the suppression of acts of aggression or other breaches of the peace, and to bring about by peaceful means, and in conformity with the principles of justice and international law, adjustment or settlement of international disputes or situations which might lead to a breach of the peace*” (Article 1, para. 2 of the United Nations Charter 1945).

Peaceful resolution of international disputes emerges as a fundamental principle at Article 2, para. 4 of the United Nations Charter, which provides that “*all Members shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any state, or in any other manner inconsistent with the Purposes of the United Nations.*” (Monserrat Filho 2007).

Additionally, the United Nations Charter regulates self-defense in Article 51, stipulating:

*Nothing in the present Charter shall impair the inherent right of individual or collective self-defence if an armed attack occurs against a Member of the United Nations, until the Security Council has taken measures necessary to maintain international peace and security. Measures taken by Members in the exercise of this right of self-defence shall be immediately reported to the Security Council and shall not in any way affect the authority and responsibility of the Security Council under the present Charter to take at any time such action as it deems necessary in order to maintain or restore international peace and security.*

Consequently, as far as defensive measures are concerned, States reserve their right of self-defense against aggressive conducts *vis-à-vis* their space objects and related space-based systems, in accordance with and within the limits provided by the United Nations Charter (Shaw 2003).

Space Law treaties, celebrated under the auspices of the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS), (Cheng 1997) also support domestic space security initiatives, as provided by its undeniable “Magna Carta,” i.e., the 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space Including the Moon and Other Celestial Bodies (“OST”).

Early in its text, said treaty specifically recognizes “*the common interest of all mankind in the progress of the exploration and use of outer space for peaceful purposes.*” Further, in accordance with Article I OST, it is stated that “*the exploration and use of outer space, including the Moon and other celestial bodies, shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development, and shall be the province of all mankind.*”

The importance of this provision to emerging space faring nations is clarified by (Masson-Zwaan and Hofmann 2019):

*This clause was included to accommodate the developing countries, united in the ‘Group of 77’, who wished to be more involved in space activities. But what exactly the term ‘province of mankind’ means is not very clear; the treaty itself provides no further hint or explanation, and its meaning is subject to debate.*

Irrespective of conflicting interpretations in relation to the definition of specific terms in the OST such as “peaceful purposes” and “province of mankind,” continuous access to, as well as exploration and use of outer space, is granted therein to all nations, provided applicable rules are observed and general interests of mankind are acknowledged.

Finally, since international responsibility for all national space activities, whether governmental or nongovernmental, contemplated by Article VI OST, domestic regulation of space activities is justified, devising proper mechanisms for authorization and supervision.

Appraising Brazilian initiatives towards space security contributes to a more comprehensive understanding of emerging space faring nations perspectives on that regard, representing a case study capable of contributing to the further development of not only domestic initiatives, related to space policy and law, but also to international cooperation mechanisms in general.

## Space Security and Emerging Space Faring Nations

The secure and sustainable access to, and use of, outer space, free from hazardous threats, is obviously important to the international community as a whole, but of particular relevance to emerging space faring nations (Space Security Index 2018). Due to insufficient technical redundancy, limited scientific capabilities, and pure economic constraints, those nations tend to experience overreliance in relation to a small selection of space assets. Therefore, whether associated with space environment or related to irresponsible or dangerous conduct from other actors, those risks are to be suitably comprehended, in order to support efficient planning and appropriate courses of action.

Around the world, developing nations look for space capabilities to secure their economic, political, and social development (Space Security Index 2018). Artificial satellites represent strategic tools to address national demands from the vantage point of Earth's orbit, supporting strategic governmental initiatives towards local concerns. Thus, through the use of space objects, it has become possible for many nations of the so-called "global South" to support continuous contact with remote locations, as well as to monitor and survey frontiers, some of which are still to be properly delimited. Urgent measures to protect fragile biomes, in face of natural disasters and ecological challenges, are often only made effective by reliance on space capabilities. As far as crucial economic activities are concerned, the exploitation of natural commodities growingly depends upon weather and remote sensing satellites.

As a *de facto* emerging space faring nation, Brazil acknowledges the crucial importance of space activities to the exercise of its national sovereignty. For a territory of 8,514,215.3 km, home of over 200 million people, appropriate satellite cover is always a challenge. Through the years, successive federal governments have invested time, capital, and people on strategic initiatives focused on local needs, ranging from remote sensing to telecommunications capabilities. Nevertheless, space activities remain an expensive endeavor, and access to crucial technology is often limited by political and legal constraints. Thus, Brazil has recognized that international cooperation is frequently required to secure specific services and expertise, leading to the negotiation of agreements with foreign partners.

Brazilian space assets are to be considered not only crucial to its national development, but even precious, irrespective of their economic worth or technological capabilities, due to the relatively remarkable efforts required for acquisition and use. Relying on an arguably insufficient satellite network, Brazilian authorities should certainly reserve more attention to space security initiatives. Nevertheless, official assessments and academic researches on the topic remain few and far between, contributing to a somewhat challenging local scenario, similar to the one faced by other emerging space faring nations.

---

### Brazilian Space Policy: An Overview

Brazilian space activities have been developed in accordance with a comprehensive and ambitious space program, first envisaged in the early 1960s. Since then, the South American giant has successfully conducted a wide range of initiatives,



contracted launching services for many “home-built” satellites and even for sending an astronaut into Earth’s orbit, in an overarching effort towards achieving complete national space autonomy (Bittencourt Neto 2011).

National launching facilities were developed in Brazilian territory, including the Alcantara Launching Center (“Centro de Lançamento de Alcântara,” CLA), designed in 1983. Strategically located in a privileged geographical region, near the Equator line (Paubel 2002), more than 200 sounding rockets have been launched from CLA (Costa Filho 2002). Due to its global position, launchings benefit from the Earth’s rotation in order to achieve greater speed, allowing fuel economy and increased payload capacity. Furthermore, space objects can be launched from CLA into equatorial and polar orbits, without passing over inhabited regions, due to its proximity to the Atlantic Ocean (Monserrat Filho 2002). The launching center’s economic potential has been recognized internationally, leading to related agreements being accorded with foreign partners such as Ukraine and USA.

A relevant number of space objects were designed and assembled in Brazil, in full or in part, usually emerging from the technological laboratories of the National Institute for Space Activities (“Instituto Nacional de Pesquisas Espaciais,” INPE), at São José dos Campos. As devised, INPE’s main mission is to produce high quality of science and technology in the space and terrestrial environment areas and to offer unique products and services for Brazilian benefit (INPE 2019).

The final segment of the Brazilian space program revolves around the development of a national launching vehicle, thus providing independent access to outer space. Named VLS (for Satellites Launching Vehicle, “Veículo Lançador de Satélites” in Portuguese), the program has faced budgetary and technical burdens since its conception, in the late 1970s. Without fruitful international cooperation, the VLS suffered from delays and complications (Paubel 2002). Despite notable constraints, several sounding rockets have successfully been conceived, most notably from series VS-30, VS-40, and VSB-30, allowing Brazilian scientists and engineers to progressively advance towards a national launching vehicle (Azevedo 2007).

International agreements, accorded with both space-faring and emerging space-faring nations, have allowed Brazil to achieve further capabilities, through joint missions involving satellites and rocketry. Important south-south partnerships have been accorded, most importantly with China, through the CBERS Program (China Brazil Earth Resources Satellites), focusing on remote sensing capabilities, which led to the joint development and launching of satellites CBERS-1 (1999), CBERS-2 (2003), CBERS-2B (2007), and CBERS-4 (2014). The latest satellite of the CBERS program was expected to be launched in December 2019 (INPE 2019).

National space activities have qualified Brazil, by fact and by law, as a Launching State, term defined by Article I, c, of the Convention on the International Liability for Damage Caused by Space Objects (LIAB), of 1972, as including those which launch or procures the launching of a space objects, as well as those from whose territory or facility a space objects is launched, irrespective of the success of its mission (Article I, c, LIAB).

To improve coordination of the Brazilian space program and stress its peaceful purposes, the Brazilian Space Agency (“Agência Espacial Brasileira,” AEB) was created by Law 8.854, of February 10, 1994. A civilian entity headquartered in

Brasilia, it enjoys financial and administrative autonomy (Article 2). AEB coordinate the efforts of INPE, especially in relation to satellites, with those of Aerospace Technical Center (Centro Técnico Aeroespacial – CTA), regarding launching vehicles and launching centers. The Brazilian space agency was conceived to improve management of the national space program, while stressing the civil inclination of its many programs and initiatives (Costa Filho 2002).

The peaceful nature of the national space program is in line with the Brazilian Constitution of 1988, which states that the country shall be governed in its international relations, inter alia, by the defense of peace, peaceful settlement of disputes and cooperation among peoples for the progress of humankind (Article 4). Indeed, Brazil has been part of several relevant disarmament instruments, including the Treaty of Tlatelolco (1967), which bans nuclear weapons in Latin America and the Caribbean, as well as Treaty on the Non-Proliferation of Nuclear Weapons (1968), of universal application. More recently, Brazil's membership in the Missile Technology Control Regime (MTCR) was approved, in 1995.

The goals and objectives of the Brazilian space program are determined by the National Program for Development of Space Activities (“Programa Nacional de Desenvolvimento das Atividades Espaciais,” PNDAE), established by Decree 1.332, December 8, 1994. Accordingly, said document clarifies that the Brazilian space program aims at fostering national capability in relation to space activities capable of addressing national concerns, while benefiting the whole local people.

In order to plan and promote the PNDAE, the National Program of Space Activities (“Programa Nacional de Atividades Espaciais,” PNAE), a periodically reviewed instrument, was contemplated. Currently in its current fourth edition, applicable to the period of 2012–2021, the PNAE stresses the peaceful purposes of the Brazilian space program. Additionally, the importance of acquiring sensitive technologies applicable to launching vehicles and satellites is mentioned, in order to obtain national space autonomy. As stated therein (Brazilian Space Agency 2012):

*The PNAE aims to enable the country to develop and use space technology in solving national problems and for the benefit of the Brazilian society, contributing to improve the quality of life, through the generation of wealth and job opportunities, improvement of scientific activities, expanding awareness of the national territory and better perception of environmental conditions.*

Emerging space faring nations often face complex barriers to develop nationally integrated space initiatives. In accordance with José (Monserrat Filho 1997), the greatest challenge faced by the Brazilian Space Program is “to raise the number of specific programs, taking advantage of growing possibilities and needs of international cooperation in the space sector, with participation of many nations.”

To overcome those difficulties, the National System for Development of Space Activities (“Sistema Nacional de Desenvolvimento das Atividades Espaciais,” SINDAE) was constituted, through Decree 1.953, of July 10, 1996, aiming at the coordination of space activities, not only between the federal bodies and entities but also with private actors (Article 3, I, II and III).

## Domestic Regulatory Instruments

As other Latin American nations, Brazil still awaits the enactment of a specific law regarding space activities, which, as per Article 22, X, of Brazilian Constitution of 1988, would be subject to federal exclusive jurisdiction. Nevertheless, reflecting the intention of opening the country to the international space market and based on CLA's potential to attract foreign partners, AEB enacted administrative edicts regulating launching activities taking place on Brazilian territory.

The referred instruments, namely, Edict 27, of June 20, 2001 (which revoked the Edict n. 8, of February 14, 2001), regarding launch licenses and Edict 5, of February 21, 2002, relating to the authorization of space launch activities on Brazilian territory, are not restricted to CLA only, enjoying vast jurisdiction. However, both edicts stress that their rules do not apply to "*space launching activities which could be carried out by Brazilian governmental organizations or bodies*" (Article 1, Paragraph 2, Edict 27/2001, and Article 1, Paragraph 2, Edict 5/2002).

As far as the Brazilian legislative structure is concerned, edicts enacted by federal autonomous organizations such as AEB are not located in a prime position; even so, they are enforceable and do provide rights and obligations, as long as there are no conflicts with superior norms (Bittencourt Neto 2009; Von der Dunk 2003). Frans G. VON DER DUNK highlighted the importance of such edicts, affirming that, with Edict 27/2001, "*Brazil became the ninth nation world-wide to establish a national space law in the narrow sense of the world – an act focusing exclusively on space activities and prominently including a system for encapsulating private participation in such activities within the State jurisdiction, international responsibilities and international liabilities.*"

On this point, more recently, the AEB Edict 120, of 26 August, 2014, approved an updated regulation on procedures and definition of the necessary requirements for the application, evaluation, dispatch, control, monitoring, and supervision of license to perform space launching activities on Brazilian territory, therefore revoking Edict 27/2001.

In addition to the referred instruments, further regulatory mechanisms were advanced, including the Space Sector Safety Regulations, issued by AEB Superior Council in 2007, applicable to space launchings conducted from Brazilian national territory. Providing technical rules and standards for execution of certain space activities, the Space Safety Regulations cover all actions encompassed from the design stages up to the operational phases. General and specific rules are defined therein dependent on the nature of the system.

According to a comprehensive set of interrelated instruments, provided by the AEB Resolution 71, of December 5, 2007, now in force, the Space Sector Safety Regulations describe the conditions to be complied with for "*the protection of people, property and the environment with respect to operations for the sending of commercial space artifacts.*" Applicable requirements include manufacturing operational processes, rocket assembly and satellite integration, launches, and environmental impact studies.

The Space Sector Safety Regulations are arranged in two volumes of rules, encompassing diverse but interconnected provisions. The first volume covers the “General Regulations for Space Safety,” while the second consists of seven different technical regulations, ranging from space safety to areas such as environmental safety, launch and flight safety, payload safety, vehicle launch complex safety, and intersite area safety. The third Volume of the Brazilian Space Safety Regulations, destined to “Accident Investigation and Prevention Regulation,” is currently under preparation by the local authorities.

The first set of regulations, provided by volume I, establishes the general safety requirements for commercial space activities in Brazil. For this reason, any entity intending to develop space activities in and from Brazilian launching centers shall meet those regulations, in mandatory bases. Likewise, the conditions agreed upon in the international instruments in force, for a foreign participation in activities from launching centers licensed by AEB, are also applicable.

The General Regulations for Space Safety addresses a total of 22 sections, supporting the topic of security certificates. In fact, it is up to the AEB to constitute or designate a government technical entity, the Space Certification Body (“SCB”), responsible for conducting the space certification processes and the issuance of the “Safety Certificates” established in the regulation. Indeed, Safety Certificates constitute the evidence of compliance with the security requirements necessary to issue applicable licenses and authorizations.

Accordingly, in the topic concerning the building and operation of a launching complex, the technical approval of the SCB project is mandatory. The applicant shall demonstrate that the engineering design meets the requirements of the Brazilian General Regulations and the Technical Regulations, including space safety, environmental safety, launch and flight safety, payload safety, launch complex safety, launching vehicle safety, and intersite area safety. After complying with the mentioned requirements, the “Launch Complex Project Safety Certificate” shall be issued by the SCB.

Moreover, said document establishes the requirement of a “Certificate of Technical and Operations Safety” for space launching activities. The Certificate shall be issued by the SCB only after the organization responsible for the launching complex demonstrates compliance with the requirements of the Technical Safety Regulations for the Launch Complex, which is in part 5 of volume 2 of the Brazilian Space Sector Safety Regulations (Superior Council of the Brazilian Space Agency 2007).

Brazil has also focused efforts on developing the “Launch Vehicle Safety Certificate of Conformity.” Again, the document must be issued by the SCB, in accordance with specific conditions. In this case, the entity responsible for the launching vehicle design shall prove that it meets the requirements of the Launching Vehicle Safety Technical Regulation. This regulation is the part 6 of volume 2 of the Brazilian Space Sector Safety Regulations (Superior Council of the Brazilian Space Agency 2007).

Any change in the design of the safety-related systems of the launching vehicle shall require the application for a new certificate, including all technical documentation, such as test and analysis memorials, material specification, descriptive

drawings, production processes, the tests, transport procedures, assembly, operation, and procedure of integrating the vehicle with the payload.

The significance granted to SCB certification procedure is illustrated by the applicant's obligation of obtaining a "Certificate of Production Compliance of the Launch Vehicle." Essentially, assembly, transportation, and integration activities of each launching vehicle can only be performed after SCB issuing of a Certificate, in order to assure the necessary safety of operations.

Regarding payload security, another certificate of conformity must be issued by the SCB on that regard. Thus, the entity responsible for each space launching, after proving that its payload meets the "Technical Regulations for Payload Safety" requirements, shall be awarded such specific certification (Superior Council of the Brazilian Space Agency 2007).

In consideration of the launching center's technical and operational safety, as found in volume 2 of the Brazilian Space Sector Safety Regulations, the launching center entity is required to hold a valid "Certificate of Technical and Operational Safety of the Launching Center."

Likewise, as reflected in other instances, the certificate will be issued by the SCB after proof of compliance with the general character of the Technical Regulations for Launch and Flight Safety (part 3, volume 2 of the Brazilian Space Sector Safety Regulations). It is worth mentioning that, according to the standards, "general" requirements of the Technical Regulation are those not directly related to a specific mission or launching.

It must be stressed that safety for space launching and flight is major concern for Brazilian authorities. In fact, the SCB shall issue a "Certificate of Safety for Space Launch and Flight" whenever it verifies that it meets the requirements of the Regulations for Launch and Flight Safety, directly related to a specific mission or launch (Superior Council of the Brazilian Space Agency 2007). Note should be granted to the fact that each launching shall require a new, additional Certificate.

Accordingly, the authorization for space launching can only be granted after the fulfillment of important provisions imposed by the Brazilian Law. The entity responsible for the space launching shall demonstrate that all applicable requirements and certificates are valid, under supervision of SCB. Indeed, it is possible to affirm that current Brazilian regulations do meet the essential safety standards for launchings from the national territory, in line with the established international instruments and guidelines. The Space Certification Body of Brazil, as provided, may follow any certification application by entities responsible for a space launching, including proof of compliance with regulations and those applications for technical approval of a component, software, or device.

One should notice that, during the certification process, SCB is entitled by law to require access to technical data, necessary to approve the entity responsible. Some important questions may arise during such process, since the public authority may demand further contact to the entity and all their suppliers, including manufacturing facilities. To properly address rights and duties, the treatment of those data should not, by any means, characterize or lead to public disclosure of trade secrets, nor impact in the related intellectual property rights.

Technical certificates issued by foreign States may be accepted by the SCB, with adoption of some procedures, such as a mutual recognition agreement, identification of rules applied to the certification process, and any applicable additional requirements, among other instances eventually appropriate to that end, as long as compatible with the Brazilian Space Sector Safety Regulations (Superior Council of the Brazilian Space Agency 2007). SCB may cancel any certificate if the risk associated with some requirement is above of acceptable levels established by Brazilian Space Safety Regulations, including situations in emergency scenarios. Finally, the holder of a certificate shall storage all data related to any fact or event that results in exposure to risks that exceeds the acceptable levels of the regulations, for possible consultation.

The new dimension brought by Internet, with the digitalization of data, can potentialize breaches and negative disclosure. It is appropriate to address, at this point, that Brazil has a new law (n. 13.709, of August 14, 2018), designed to foster data security and protection (Brazil 2019). In this context, the Space Safety Regulations in Brazil also allows international agreements, which Brazil is part of, to provide access to data. Essentially, we consider that is very important to establish international channels to exchange data between States and companies working with the development, launch, and operation of satellites.

The before mentioned law, known as the General Personal Data Protection Act (LGPD), which will come into force in 2020, is intended to regulate the processing of personal data of customers and users by public and private companies, with important topics on international data transfer and data security, a sensitive issue as far as specific space activities are concerned.

The Brazilian “Data Law” applies to any processing operation carried out by a legal entity of public or private law, irrespective of the country in which its headquarter is located or the country where the data sits. On this regard, one should notice that international transfer of personal Brazilian data shall only be allowed to countries or international organizations capable of providing a level of protection deemed adequate in accordance to the provisions of the Brazilian Law. Additionally, international transfer of personal data is authorized when resulting in a commitment undertaken through international cooperation, therefore eventually encompassing space cooperation agreements.

---

## **Brazilian Space Situational Awareness Initiatives**

In order to better protect its national space objects against potential threats, Brazil has been developing space situational awareness initiatives, including through international cooperation. Space Situational Awareness (SSA) has been defined as “*the comprehensive knowledge of space objects and the ability to track, understand and predict their future location,*” in accordance with the Space Generation “Space Safety & Sustainability Working Group” (2012).

The purpose of SSA initiatives is to safeguard space-based systems, currently recognized as fundamental assets to the sustainable development of every nation.

Nowadays, those actions are of particular relevance since, as observed by (Bobrinsky and Del Monte 2010), *“the destruction of even part of space infrastructure can have heavy consequences for the safety of citizens and economic activities.”* For emerging space faring nations like Brazil, understanding potential threats to their satellites and related space-based systems is highly advised, considering the difficulties involved in supporting strategic orbital capabilities.

The major concerns of SSA initiatives may be summarized as including, first and foremost, tracking and surveillance of space objects, since the increasing population of space debris represents relevant risks of in-orbit collisions and interferences. Also, space weather capabilities are taken into consideration, due to the fact that solar storms and explosions of charged particles can seriously damage space objects and power grids on Earth. Finally, near-earth objects, i.e., small natural bodies attracted by Earth’s gravitational field, are of particular interest for representing orbital or terrestrial dangers.

Thus, improved awareness of the space environment is important to secure safe and continuous development of space activities. For an emerging space faring nation as Brazil, those initiatives may be considered even more relevant, providing information necessary to address potential threats to the continuous service of operational space objects.

In 2007, the Brazilian National Institute for Space Research (INPE) assembled a task force named EMBRACE, acronym for Brazilian Studies and Monitoring of Space Weather (*“Estudo e Monitoramento Brasileiro de Clima Espacial,”* in Portuguese), which culminated in the establishment of an official space weather program. EMBRACE’s objective is *“to monitor the Solar-Terrestrial environment, the magnetosphere, the upper atmosphere and the ground induced currents to prevent effects on technological and economic activities.”*

The relevance of space weather initiatives is clarified by (Pelton 2013), who explains that *“solar flares and coronal mass ejections (CMEs) could be much larger problems than previously thought with modern electronic and electrical systems particularly at risk.”*

EMBRACE is financed by the main governmental funding agencies, including the National Council for Scientific and Technological Development (CNPq), the São Paulo Research Foundation (FAPESP), the Brazilian Innovation Agency (FINEP), and the Brazilian Ministry of Science, Technology, Innovation and Communication (MCTI). Such support clarifies how decisive and strategic space weather monitoring has been recognized by local public authorities. Currently, EMBRACE is the official interlocutor of Brazil in space weather at the World Meteorological Organization (WMO).

As far as space debris are concerned, the Brazilian National Laboratory of Astrophysics (*“Laboratório Nacional de Astrofísica,”* LNA), with support from the Brazilian Space Agency, celebrated an agreement with the Russian Space Agency (ROSCOSMOS) to install a specialized telescope in the Pico dos Dias, Brazópolis. Strategically located in the Southern Hemisphere, it enhanced Russian space situational awareness capabilities, while also granting access to Brazilian authorities regarding potential threats represented by man-made derelict, or uncontrolled space objects, including their related parts, to national satellites.

Recently, the Brazilian Ministry of Defense signed, in December 12, 2018, a Space Situational Awareness (SSA) agreement with USA Defense Department, as part of a larger effort to increase safety of space operations. Data cross-check among applicable parties provides essential support for space activities, such as satellite launching and decommissioning, satellite maneuver planning, support for in-orbit anomalies, electromagnetic interference investigation, and in-orbit conjunction assessments (Barreto 2019).

As Brazilian space activities naturally evolve, and more national space objects are launched in orbit, further space situational awareness initiatives will be required, whether developed with autochthony or under international cooperation agreements. Commons goals and concerns may in fact lead to the development of regional and even global initiatives, based on further synergies among the involved parties.

---

## Prevention of Arms Race in Outer Space: Brazilian Perspectives

Brazilian delegations have, at least until recently, sustained a consistent positioning at the United Nations Conference on Disarmament (CD), in Geneva, as far as the topic of prevention of an arms race in outer space (PAROS) is concerned. Alternate governments and regimes in the country did not impair Brazilian engagement in debates, denouncing growing concern in relation to the weaponization of outer space.

As explained by (Tronchetti 2013), *“due to the increasing importance of space assets and the consequent need to protect them, there is a widespread concern that states might eventually weaponize outer space. Considering that the space treaties do not impose with any substantial limit to such a weaponization, initiatives aimed at creating legal barriers to such an option have been launched.”*

Debates on PAROS at CD dates back to the early 1980s, gaining traction after the establishment of a specific ad hoc committee in 1985, designed to *“to examine as a first step at this stage, through substantive and general consideration, issues relevant to the prevention of an arms race in outer space”* (Conference on Disarmament, Report of the Ad Hoc Committee on Prevention of an Arms Race in Outer Space, document CD/642, December 4, 1985, para. 1).

More recently, in accordance with the United Nations General Assembly Resolution 72/250, of 2017, on further practical measures for the prevention of an arms race in outer space, the Secretary-General appointed a Group of Governmental Experts from 25 Member States, including Brazil. At its first session, the Group elected the Brazilian Ambassador Guilherme de Aguiar PATRIOTA as its chair, leading its sessions in Geneva.

The latest report of the Group of Government Experts on further practical measures for the prevention of an arms race in outer space was presented by the chair in 2019, informing about the meetings, devoted to interactive discussions and share of views on the following topics: the existing legal regime in outer space and elements of general principles; elements of general obligations; elements related to monitoring, verification, and transparency and confidence-building measures; and elements related to international cooperation, institutional arrangements and final provisions (A/74/77, p. 7).



The group was guided by an indicative timetable, prepared to focus discussions on various thematic areas considered of relevance, including the international security situation, existing legal regime applicable to the prevention of an arms race in outer space and the application of the right of self-defense in outer space (A/74/77, pp. 8–9).

Regarding other intergovernmental initiatives related to the prevention of an arms race in outer space, reference should be made to the Brazilian position on the European Union's Draft International Code of Conduct for Outer Space Activities. A draft text was first presented to the international community in 2012 as an independent and ad hoc initiative, not related to debates at CD.

Brazil presented, at the time, serious reservations in relation to the Code of Conduct, most importantly for the fact that the document was not widely and openly discussed at the CD or COPUOS, and that it did lack legitimacy due to the fact that countries from other continents, such as Brazil, did not have opportunity to discuss or propose amendments. Debates in relation to the Code of Conduct have lost momentum with time, including among Brazilian officials.

---

## Conclusions

Emerging space faring nation are increasingly concerned with the development of space security initiatives. Brazil, a Latin American country with a long-standing space program, which lead to the development of many space objects, two launching centers and aims at the development of a national launching vehicle, cannot be left out of the debates on this subject matter.

Indeed, among various international fora, Brazil has presented its contribution to the discussions, with relevant engagement at the United Nations. Domestically, various normative instruments and guidelines have been enacted regarding important space security aspects, although still in a sparse and somewhat complex formulation. The enactment of a national federal law on space activities, contemplating space security provisions, is certainly advised.

Space situational awareness capabilities are certainly important in our days to support the continuous operation of valuable space-based assets, providing significant space security advantages. Whether via national initiatives or, even more importantly, through international cooperation, initiatives are to be continuously by the Brazilian Space Agency to the furtherance of its space program.

Multilateralism allows States, in international relations, to reduce coordination costs, while achieving greater legitimacy, thus supporting global governance. As a global concern, space security benefits from open international exchanges, reflecting national concerns and regional perspectives.

International cooperation remains a fundamental cornerstone for the peaceful development of space activities and, as such, should never be taken for granted. For an emerging space faring nation as Brazil, multilateral collaboration with foreign partners should be perceived, as well mentioned by (Forman 2002), as “*no longer a choice. It is a matter of necessity, and of fact.*”

## References

- Azevedo JLF (2007) A Capacidade Brasileira de Acesso ao Espaço. Espaço Brasileiro, a. 1, n. 2, Brasília, Brazil, March, April, May, 2007, pp 15–17
- Barreto, Andréa (2019) US and Brazil Share Information on Space. Available at: <https://dialogo-amicas.com/en/articles/us-and-brazil-share-information-space>, accessed on 24 October, 2019
- Bittencourt Neto Olavo de O (2009) Private launching activities on Brazilian territory: current legal framework. *Z Luft- Weltraumrecht* 58(3):429–449. Cologne
- Bittencourt Neto Olavo de O (2011) *Direito Espacial Contemporâneo*. Juruá, Curitiba
- Bobrinsky N, Del Monte L (2010) The space situational awareness program of the European Space Agency. *Kosm Issled* 48(5):402–408
- Brazil (2019) General Personal Data Protection Act. Law n. 13.709/2018. Available at: [http://www.planalto.gov.br/ccivil\\_03/\\_ato2015-2018/2018/lei/L13709.htm](http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm), accessed on 23 October, 2019
- Brazilian Space Agency (2012) Programa Nacional de Atividades Espaciais: PNAE: 2012 – 2021. Agência Espacial Brasileira. Brasília: Ministério da Ciência, Tecnologia e Inovação, Agência Espacial Brasileira, 2012
- Brazilian Space Agency (2020) The Embrace Program. Available at: <http://www3.inpe.br/50anos/english/presentation.php>, accessed on January 30, 2020
- Brazilian Space Agency (2020) Acordo entre Brasil e Rússia garante monitoramento de lixo espacial. Available at: <http://portal-antigo.aeb.gov.br/acordo-entre-brasil-e-russia-garante-monitoramento-de-lixo-espacial/>, accessed on January 30, 2020
- Brazilian National Institute for Space Research (INPE) (2019) Half a century conquering the space to care for Earth. Available at: <http://www3.inpe.br/50anos/english/presentation.php>, accessed on September 22, 2019
- Casella PB (2009) *Direito Internacional dos Espaços*. Atlas, São Paulo
- Cheng B (1997) *Studies in international space law*. Clarendon Press, Oxford, UK
- Committee on Prevention of an Arms Race in Outer Space Conference on Disarmament (1985). Report of the Ad Hoc Committee on Prevention of an Arms Race in Outer Space, document CD/642, December 4, 1985
- Costa Filho E (2002) *Política Espacial Brasileira*. Revan, Rio de Janeiro
- European Union (2014) Draft International Code of Conduct for Outer Space Activities, Version March 31, 2014
- Forman S (2002) *Multilateralism and US foreign policy: ambivalent engagement*. Lynne Rienner, London
- Masson-Zwaan T, Hoffmann M (2019) *Introduction to space law*, 4th edn. Kluwer, Alphen aan den Rijn
- Monserrat Filho J (1997) *Introdução ao Direito Espacial*. SBDA, Rio de Janeiro
- Monserrat Filho J (2002) Brazilian launch licensing and authorizing regimes. *Capacity Building in Space Law – UN/IIASL*, The Hague
- Monserrat Filho J (2007) *Direito e Política na Era Espacial*. Vieira & Lent, Rio de Janeiro
- Paubel EFC (2002) *Propulsão e Controle de Veículos Aeroespaciais: uma Introdução*. UFSC, Florianópolis
- Pelton JN (2013) *Space debris and other threats from outer space*. Springer, Dordrecht
- Rosenau J (1992) *Governance without government: order and change in world politics*. Cambridge University Press, Cambridge, UK
- Shaw M (2003) *International law*, 5th edn. Cambridge University Press, Cambridge, UK
- Space Safety & Sustainability Working Group (2012) *Space situational awareness*. SSS educational series. Available at: [https://www.agi.com/resources/educational-alliance-program/curriculum\\_exercises\\_labs/SGAC\\_Space%20Generation%20Advisory%20Council/space\\_situational\\_awareness.pdf](https://www.agi.com/resources/educational-alliance-program/curriculum_exercises_labs/SGAC_Space%20Generation%20Advisory%20Council/space_situational_awareness.pdf). Accessed on 25 Oct 2019
- Tronchetti F (2013) *Fundamentals of space law and policy*. Springer, Dordrecht
- Von Der Dunk, FG (2003) Launching Alcântara into the global space economy – the 2001 Brazilian National Space Law. *Revista de Direito Aeronáutico e Espacial – SBDA*, n. 86, Rio de Janeiro, p 23
- Weeden B (2018) *Space security index 2018*, 15th edn. Waterloo, Waterloo Printing



# Space and Security Activities in Azerbaijan **36**

Tarlan Mammadzada

## Contents

Introduction .....	668
Azercosmos: the Satellite Operator of Azerbaijan .....	670
Satellite Imagery Sources and Analysis Methodology .....	672
Results of Satellite Imagery Analysis .....	674
Environmental Damage .....	674
Permanent Infrastructure Changes .....	675
Exploitation and Pillage of Natural Resources .....	679
Destruction of Public and Private Property, Including Historical and Cultural Heritage ...	682
Exploitation of Agricultural and Water Resources .....	687
Implantation of Settlers and Construction of Permanent Social Infrastructure .....	694
Conclusion .....	697
References .....	698

## Abstract

Earth observation satellites are the source of valuable data for military intelligence, strategic planning, and development. Azerbaijan continuously monitors its occupied territories by means of remote sensing techniques. These territories constitute 20% of Azerbaijan, including the Nagorno-Karabakh region, the seven adjacent districts, and some exclaves. Despite the resolutions, adopted by UN Security Council in 1993, which reaffirmed the Nagorno-Karabakh region as a part of Azerbaijan and called for immediate, complete, and unconditional withdrawal of the occupying forces from all territories of Azerbaijan, the occupant still continues its activities, which lead to catastrophic changes in the occupied areas.

---

T. Mammadzada (✉)  
“Azercosmos” OJSCo, Baku, Azerbaijan  
e-mail: [tarlan.mammadzada@azercosmos.az](mailto:tarlan.mammadzada@azercosmos.az)

Azerbaijan owns a high-resolution Earth observation satellite Azersky, which in constellation with SPOT 6 is used to continuously monitor these areas, revealing the unacceptable changes of physical, economic, demographic, and cultural character in the occupied territories, such as environmental damage, permanent infrastructure changes, exploitation and pillage of natural resources, destruction of public and private property, implantation of settlers, and construction of permanent social infrastructure.

This chapter contains information about the remote sensing capabilities and techniques, as well as high-resolution satellite imagery, acquired by “Azercosmos” OJSCo, the satellite operator of Azerbaijan, which provides the overview of activities in the occupied territories of Azerbaijan from space.

---

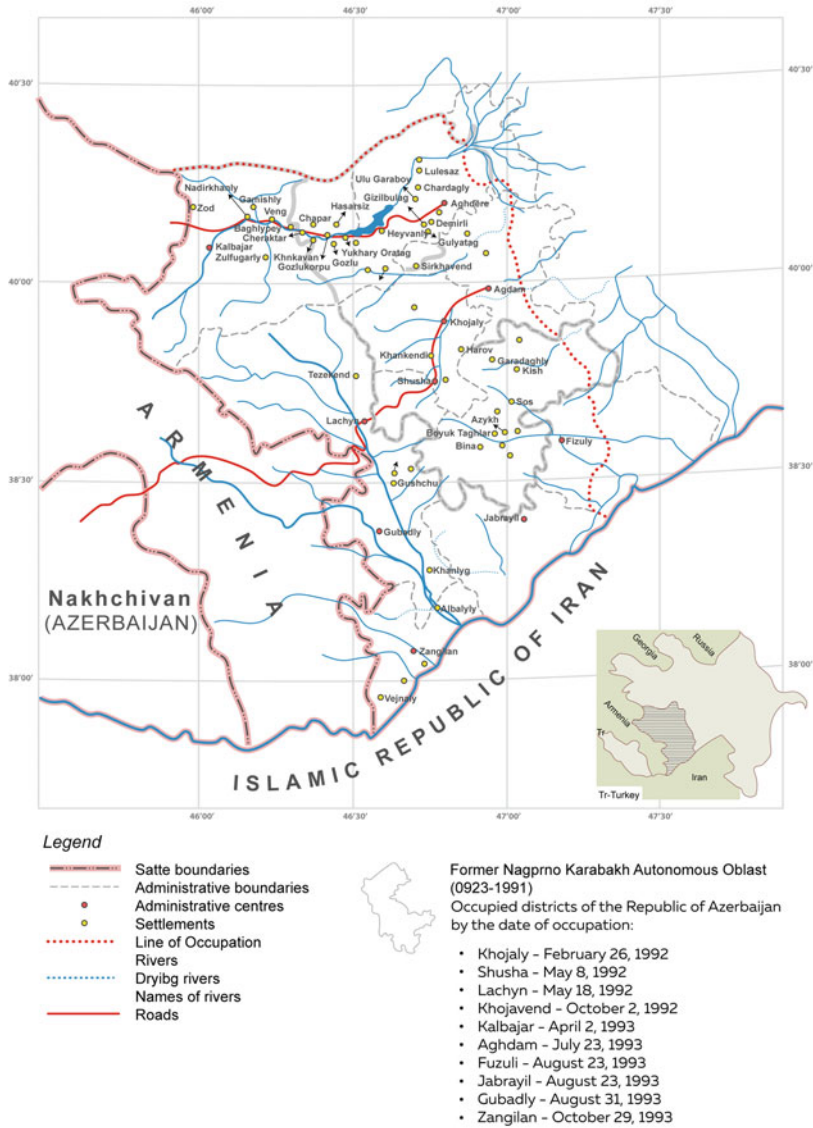
## Introduction

Satellite imagery, from the very beginning, seems to have found its main domain of application in the military field and until today has been used mostly for military strategic planning, intelligence, and development (Van Persie et al. 2000). It is essential, for military purposes, to have an accurate representation of a specific zone of interest anywhere in the world. According to Euroconsult, the leading global consulting firm specializing in space, military is the largest consumer of remote sensing data (more than 60% of all data) (Euro consult Research 2012).

This is particularly important for Azerbaijan, which has 20% of its territories occupied by Armenia, including the Nagorno-Karabakh region, the seven adjacent districts, and some exclaves (Fig. 1). The fact of the occupation of the territories of Azerbaijan using military forces has been consistently deplored by the international community. In 1993, the UN Security Council adopted resolutions 822 (1993), 853 (1993), 874 (1993), and 884 (1993), condemning the use of force against Azerbaijan and the occupation of its territories and reaffirming the sovereignty and territorial integrity of Azerbaijan and the inviolability of its internationally recognized borders. In these resolutions, the Security Council concluded that the Nagorno-Karabakh region is part of Azerbaijan and called for immediate, complete, and unconditional withdrawal of the occupying forces from all occupied territories of Azerbaijan. (See UN Doc. A/67/875–S/2013/313, 24 May 2013.) However, the occupant disregards the international community to this day, continuing to violate international law.

Azerbaijan owns an Earth observation satellite Azersky (formerly SPOT-7), operated by “Azercosmos” OJSCo (hereafter referred to as Azercosmos) since 2014. This satellite orbits regularly over the occupied region, producing high-resolution images of huge areas. Using this satellite, Azerbaijan continuously monitors its occupied territories, observing unacceptable catastrophic changes.

The activities in the occupied territories of Azerbaijan are leading to permanent changes in the economic, physical, cultural, and demographic character of the occupied territories, which was also confirmed by Organization for Security and Co-operation in Europe (OSCE) missions in the occupied territories in 2005 and 2010 (Since 1992 the Organization for Security and Cooperation in Europe (OSCE)



**Fig. 1** The occupied territories of the republic of Azerbaijan

has engaged in efforts to achieve a settlement of the conflict under the aegis of its Minsk Group, currently under the co-chairmanship of the French Republic, the Russian Federation and the United States of America; See “Letter of the OSCE Minsk Group Co-Chairs to the OSCE Permanent Council on the OSCE Minsk Group Fact-Finding Mission (FFM) to the occupied territories of Azerbaijan Surrounding Nagorno- Karabakh (NK)”, UN Doc. A/59/747–S/2005/187, 21 March

2005, annex I, pp. 4 and 5. For the Executive Summary of the OSCE field assessment mission report and Press release of the Ministry of Foreign Affairs of the Republic of Azerbaijan, UN Doc. A/65/801–S/2011/208, 29 March 2011.). The Ministry of Foreign Affairs of the Republic of Azerbaijan produced a report “Illegal Economic and Other Activities in the Occupied Territories of Azerbaijan” in 2016 (hereafter referred to as the “2016 Report”), which presented well-documented evidence of dramatically expanding illegal activities in the occupied territories. In 2019 Azercosmos jointly with the Ministry of Foreign Affairs of Azerbaijan published the book “Illegal Activities in the Territories of Azerbaijan under Armenia’s Occupation: Evidence from Satellite” (hereafter referred to as the “2019 Report”), where the illegal activities in the occupied territories were demonstrated by means of satellite imagery.

The present chapter contains the information about the remote sensing technologies and techniques, as well as high-resolution satellite imagery of the occupied territories, which provides sufficient and convincing evidence of ongoing activities in the occupied territories. The key findings of “2016 Report” and “2019 Report” also presented here to provide overall context in the following areas:

1. Environmental damage
2. Permanent infrastructure changes
3. Exploitation and pillage of natural resources
4. Destruction of public and private property, including historical and cultural heritage
5. Exploitation of agricultural and water resources
6. Implantation of settlers and construction of permanent social infrastructure

---

## **Azercosmos: the Satellite Operator of Azerbaijan**

Azercosmos – the national satellite operator of Azerbaijan – was established in 2010 to provide satellite-delivered telecommunication and Earth observation services to customers in both the public and the private sectors. It strives to establish Azerbaijan as one of the driving forces of the global space industry and is committed to providing customized solutions based on advanced technologies for peace and prosperity. The activities of Azercosmos are carried out in five main directions: supporting the socioeconomic development of Azerbaijan, supporting national security, expanding commercial activities, supporting space R&D activities, and representing the country in the international space arena. Azercosmos operates three satellites: two telecommunication satellites, Azerspace-1 and Azerspace-2, and the Earth observation satellite, Azersky.

In February 2013 Azercosmos launched its first telecommunication satellite – Azerspace-1, which was manufactured by Orbital Sciences Corporation. Located at 46° East longitude, the satellite has a wide coverage area including Europe, Africa, Central Asia, and the Middle East. It is designed to provide broadcasting and

telecommunications services and create platforms to meet government and corporate customers' demands.

In December 2014, within the framework of the strategic partnership with Airbus DS, Azercosmos took over the rights to operate and commercialize SPOT-7 (later rebranded to Azersky), a high-resolution optical Earth observation satellite, and started its commercial activities. Azersky acquires direct and unlimited high-resolution satellite imagery from any part of the world on a daily basis. Azercosmos has been carrying out projects for the stimulation of Earth observation services in Azerbaijan and a number of Commonwealth of Independent States (CIS) countries. Within these projects, both independent researchers and organizations, engaged in research activities, are provided with satellite imagery obtained via Azersky free of charge to implement their innovative, scientific research covering areas such as geography, dendrology, botany, zoology, soil science, and agrochemistry.

In September 2018, Azercosmos launched its third satellite – Azerspace-2. Built for Azercosmos by Space Systems Loral (SSL), Azerspace-2 is a telecommunication satellite with a 35 Ku-band active transponder payload. The satellite enhances the capacity, coverage area, and spectrum of service offerings of Azercosmos to support the demand for government and network services in Europe, Central and South Asia, the Middle East, and Sub-Saharan Africa. Azerspace-2 is ideally designed for smaller antenna and has cross connectivity between East, West, and Central Africa, as well as Europe and Central Asia.

Besides their direct commercial benefits, satellite projects also serve as the basis for the transfer of advanced technologies to the country and acquisition of knowledge, skills, and practices for the independent implementation of space-related projects as a next step. To share accumulated experience and grow the knowledge and skills necessary for the development of satellite components in Azerbaijan in the years to come, Azercosmos, together with the Ministry of Education of the Republic of Azerbaijan, annually holds CanSat Azerbaijan satellite modeling competition. Furthermore, the rocket modeling festival – Rocketry Azerbaijan – that took place within CanSat competition in April 2019 was the first of its kind in the country, where students of top local technical universities were involved in the design and launch of rocket models at the Main Satellite Ground Control Station of Azercosmos. Azercosmos was one of the main partners to hold the international ActInSpace Hackathon, organized by The National Centre for Space Studies (CNES) and European Space Agency (ESA), in Baku for the first time in 2018. Considering students' great interest to innovative projects, Azercosmos organized the NASA Space Apps Challenge in Azerbaijan in October 2019, aiming to engage coders, scientists, designers, technologists, and space enthusiasts in developing innovative solutions to NASA's toughest challenges.

The Research and Development Center of Azercosmos conducts scientific research in the field of space and astronautics. The Center develops various software for the satellite operations; conducts research on automatic recognition of objects and changes on satellite imagery through artificial intelligence techniques; and designs small satellites, small launchers, and unmanned aerial vehicles. Moreover, the team of the Research and Development Center of Azercosmos successfully

solved the assigned task at the Global Trajectory Optimization Competition and made the top 20 in June 2019.

Azercosmos officially represents the Republic of Azerbaijan at the United Nations Committee on the Peaceful Uses of Outer Space (UN COPUOS), the International Telecommunications Satellite Organization (ITSO), the European Telecommunications Satellite Organization (EUTELSAT), and International Organization of Space Communications (INTERSPUTNIK). It is also a member of the International Astronautical Federation (IAF), EMEA Satellite Operators Association (ESOA), World Teleport Association (WTA), and Smart Africa Alliance. Azercosmos is actively involved in a wide variety of international space-related projects with government, industry, and academia of Asian, European, African, and North and South American countries aimed at using outer space for peaceful purposes. Furthermore, in order to increase engagement within international organizations and support global activities in the space environment, Azercosmos became a member of the Advisory Committee of the European Telecommunications Satellite Organization (EUTELSAT IGO) in April 2019 and joined the Space Climate Observatory (SCO) initiative in June 2019. Azercosmos attaches a great importance to the development and strengthening of bilateral relations. For instance, in July 2018 Azercosmos and the National Center for Space Research (CNES) of the French Republic signed a framework agreement on space cooperation, and in February 2020 Azercosmos and the Italian Space Agency signed a memorandum of understanding on the use of outer space for peaceful purposes.

On October 25, 2019, during the elections held at the General Assembly of the International Astronautical Federation in the capital city of the United States, Washington, D.C., Baku has got the right to host the International Astronautical Congress (IAC) in 2022. Singapore, Rio de Janeiro, and New Delhi were among the bidding candidate cities to host this prestigious event.

---

## Satellite Imagery Sources and Analysis Methodology

Development of Earth observation technologies and techniques is a matter of high priority for the government of Azerbaijan. On November 15, 2018, the “State Program for the Development of Earth Observation Satellite Services in the Republic of Azerbaijan for 2019–2022” was approved by the president of Azerbaijan. The main goal of the state program is to support the socioeconomic and technological development of Azerbaijan through the application of remote sensing services. The program creates opportunities for development of the latest technologies in various areas, such as defense and security, agriculture, environmental protection, urban planning, emergency response, exploration of natural resources, maritime surveillance, and cartography.

Azersky is placed on the sun-synchronous orbit in constellation with SPOT 6, providing daily revisit over the occupied region. The high-resolution optical instrument consists of panchromatic band (0.45–0.75  $\mu\text{m}$ ) and four multispectral bands, red (0.62–0.69  $\mu\text{m}$ ), green (0.53–0.60  $\mu\text{m}$ ), blue (0.45–0.52  $\mu\text{m}$ ), and near-infrared



(0.76–0.89  $\mu\text{m}$ ), and is able to acquire up to 3 million  $\text{km}^2$  area daily with a resolution of 1.5 m suitable for 1:25,000 scale topographic mapping, wide coverage capacity of 60 km swath width at Nadir, and location accuracy of 10 m (CE90) (Fig. 2).

The cooperation with Airbus DS also includes operations of SPOT 6 high-resolution (1.5 m imagery) optical Earth observation satellite. SPOT 6 and Azersky are twin satellites that compose a constellation operating on the same orbit and phased  $180^\circ$  from each other. This orbit phasing allows the satellites to revisit any point on the globe daily, which is very effective for anticipating risks and covering large areas (Table 1).

In addition, the ground segment, constructed in Azerbaijan, allows to access images of Pleiades 1A and 1B, very high resolution (0.5 m imagery) optical Earth observation satellites of Airbus Defence and Space. This satellite constellation provides the opportunities for many applications and specifically for security, providing the latest images within an unprecedented time frame.

The analysis of the images is performed using various digital change detection methods, which aim to detect differences in the state of objects on the images over time. There are two mainly used techniques, the traditional/classical pixel-based, which employs an image pixel as a fundamental unit of analysis, and object-based, which emphasizes creating image objects and then using them for further analysis. Pixel-based technique includes the following approaches:

**Fig. 2** Azersky, high-resolution Earth observation satellite © [airbus.com](http://airbus.com)



**Table 1** Satellites viewing angles

Viewing angle	SPOT 6 or Azersky only	SPOT 6 and Azersky
<5 degrees	26 days	13 days
<20 degrees	7 days	4 days
<30 degrees	5 days	2 days
<45 degrees	2 days	1 day

- Direct comparison (image differencing, image rationing, regression analysis)
- Transformation from image (vegetation index differencing, change vector analysis, etc.)
- Classification based (post-classification comparison, multi-date direct comparison)
- Machine learning (AI network, support vector machine, decision tree)
- GIS (GIS integration)
- Advanced methods (spectral mixture analysis, fuzzy change detection, multi-sensor data fusion)

Object-based classification is performed in the following ways:

- Direct object comparison based (objects extracted from one image and then assigned to or searched from image data from second acquisition)
- Object classification comparison based (two segmentation created separately and compared)
- Multi-temporal object change detection (stacked bi-temporal images)

The changes may be detected also due to the differences in illumination, atmospheric conditions, sensor calibration, ground moisture conditions, and other effects. These factors also should be considered and corrections should be implemented (Deer 1995; Hussain et al. 2013).

---

## Results of Satellite Imagery Analysis

### Environmental Damage

The forest cutting and the predatory exploitation of natural resources in the monitored areas are seriously affecting the environment, which leads to the disappearance of various species of trees and millions of tons of tailings in tailing dumps across the occupied territories. The pollution of the territories and damage to the ecosystem is also resulted by the leaks from tailing dumps and ponds at the mining sites. Ferocious exploitation of farmlands in the occupied territories for decades has led to their extreme depletion. (See Section XV (Cutting of rare species of trees for timber and other damage to the environment) of the Report of the Ministry of Foreign Affairs of the Republic of Azerbaijan (2016).)

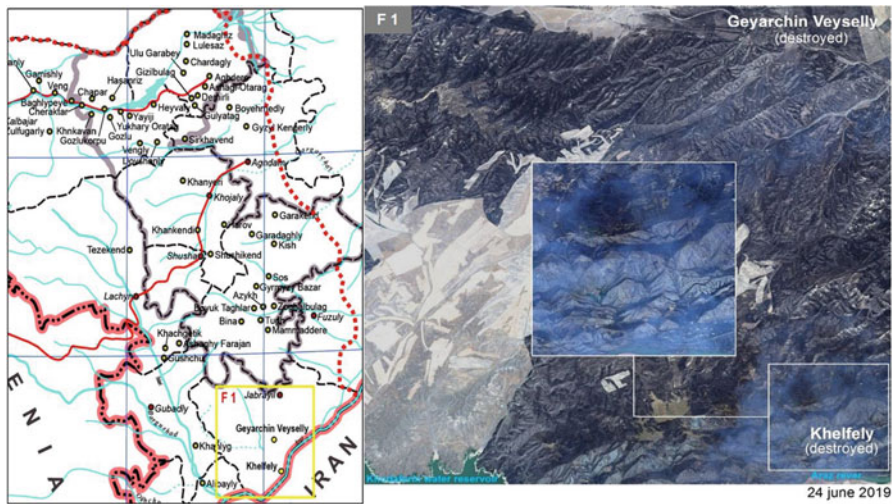
The following examples of environmental damage are presented:

- Burned area affecting villages of the occupied Jabrayil district (39° 12' 32" N, 46° 59' 11" E)
- Burned area affecting villages of the occupied Fizuli district (39° 36' 07" N, 47° 08' 44" E)

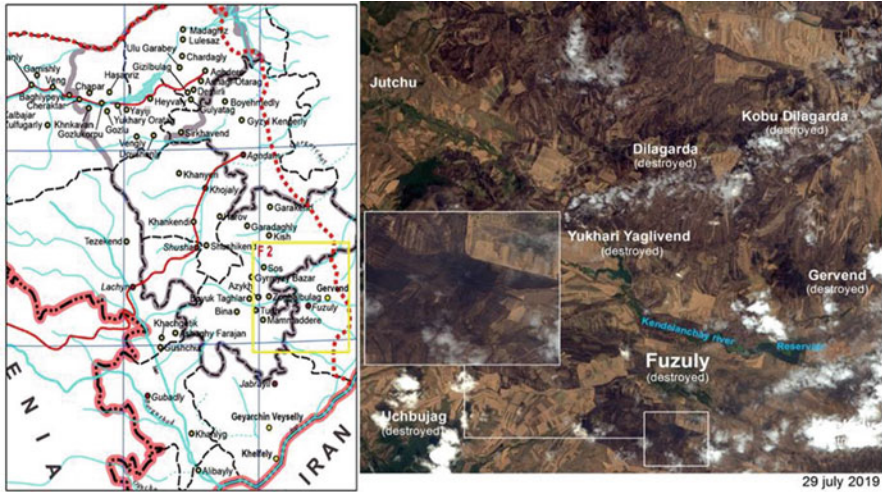
- Tailing dump caused by exploitation of Gyzybulag underground copper-gold mine near Heyvaly village in the occupied Kalbajar district ( $46^{\circ} 35' 43.645''$  E,  $40^{\circ} 8' 34.632''$  N)
- Burned area covering  $26 \text{ km}^2$  affecting Jilan and Bunyadli villages of the occupied Khojavand district and Khalafly, Khybyarli, Kurds, and Qarar villages of the occupied Jabrayil district ( $39^{\circ} 28' 29.04''$  N,  $46^{\circ} 47' 18.24''$  E)
- Forest cutting for construction of water canal near the Sarsang Water Reservoir in the occupied part of the Tartar district ( $46^{\circ} 30' 30.882''$  E,  $40^{\circ} 8' 45.486''$  N)
- Expansion of tailing dump caused by exploitation of Demirli open-pit copper molybdenum mine near Demirli, Gulyatag, and Janyatag villages in the occupied part of the Tartar district ( $46^{\circ} 46' 16.713''$  E,  $40^{\circ} 9' 2.801''$  N)
- Deforestation caused by mining activities near Chardagly village in the occupied part of the Tartar district ( $46^{\circ} 41' 33.965''$  E,  $40^{\circ} 14' 9.393''$  N)
- Burned area covering  $347 \text{ km}^2$  and affecting 25 villages in the occupied Fuzuli district stretching 22 km from the South to the North and 17 km from the East to the West ( $39^{\circ} 36' 24.92''$  N,  $47^{\circ} 06' 26.71''$  E) (Figs. 3, 4, 5, 6, 7, 8, 9, and 10)

## Permanent Infrastructure Changes

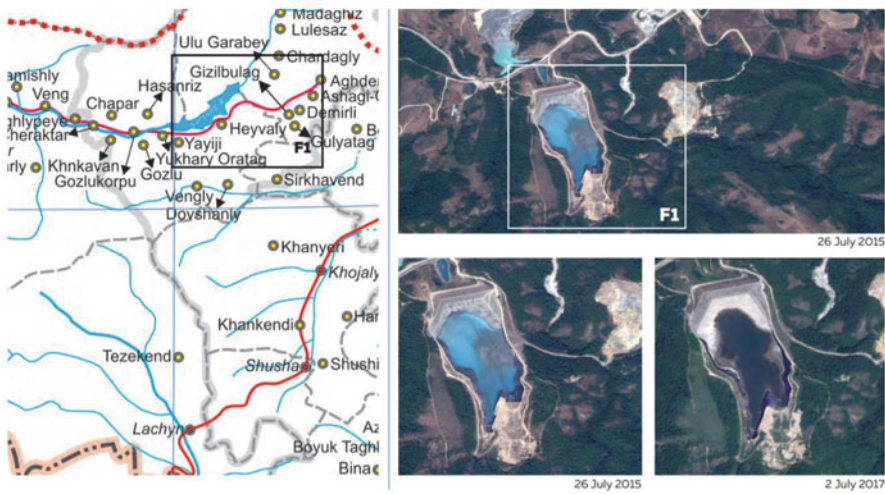
The changes in social, energy, agriculture, and transport infrastructure, including the construction of irrigation networks, roads, electrical transmission lines, water supply systems and other economic and social facilities, including the construction and reconstruction of network of roads, which are linked to the supporting of settlements in the occupied territories, are continuously monitored. (See Section XII (Extensive



**Fig. 3** Burned area affecting villages of the occupied Jabrayil district ( $39^{\circ} 12' 32''$  N,  $46^{\circ} 59' 11''$  E)



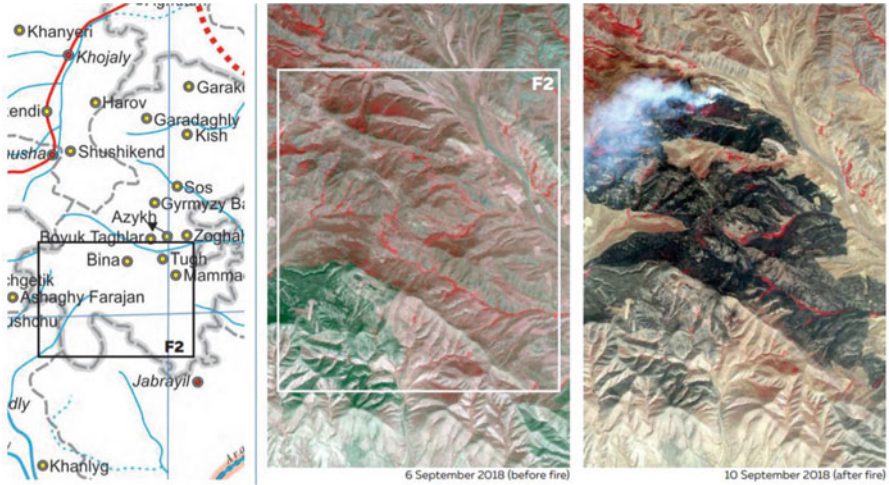
**Fig. 4** Burned area affecting villages of the occupied Fizuli district (39° 36' 07" N, 47° 08' 44" E)



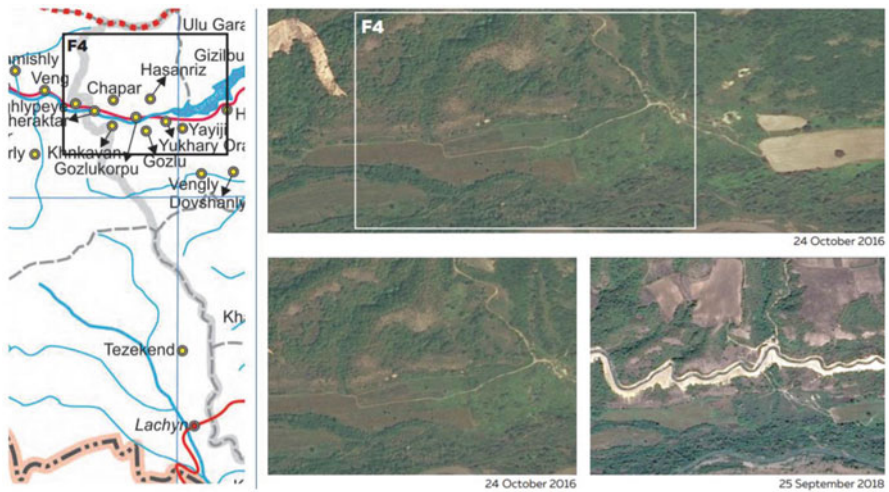
**Fig. 5** Tailing dump caused by exploitation of Gyzybulag underground copper-gold mine near Heyvaly village in the occupied Kalbajar district (46° 35' 43.645" E, 40° 8' 34.632" N)

exploitation of agricultural and water resources) of the Report of the Ministry of Foreign Affairs of the Republic of Azerbaijan (2016). Obviously, this infrastructure allows the occupant to pervasively control the entire economic and commercial system in the territories, including maintaining and supporting the economic resources and trade flows.

The following examples of permanent infrastructure changes are presented:

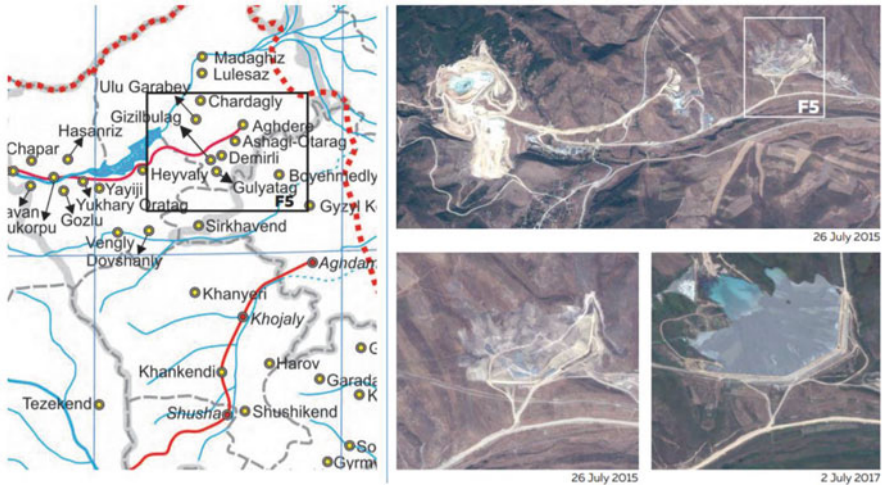


**Fig. 6** Burned area covering 26 km<sup>2</sup> affecting Jilan and Bunyadi villages of the occupied Khojavand district and Khalafly, Khybyarli, Kurds, and Qarar villages of the occupied Jabrayil district (39° 28' 29.04" N, 46° 47' 18.24" E)

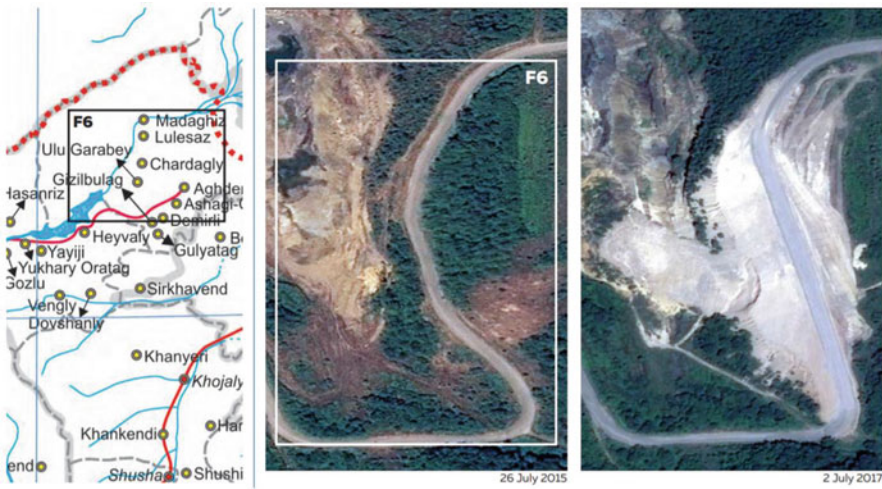


**Fig. 7** Forest cutting for construction of water canal near the Sarsang Water Reservoir in the occupied part of the Tartar district (46° 30' 30.882" E, 40° 8' 45.486" N)

- Reconstruction of Goris (Armenia)–Khankandi road passing through the occupied Lachyn district (39° 36' 17" N, 46° 32' 43" E)
- Construction of Vardenis (Armenia)–Aghdara highway passing through the occupied Kalbajar district (40° 13' 18" N, 45° 58' 59" E)

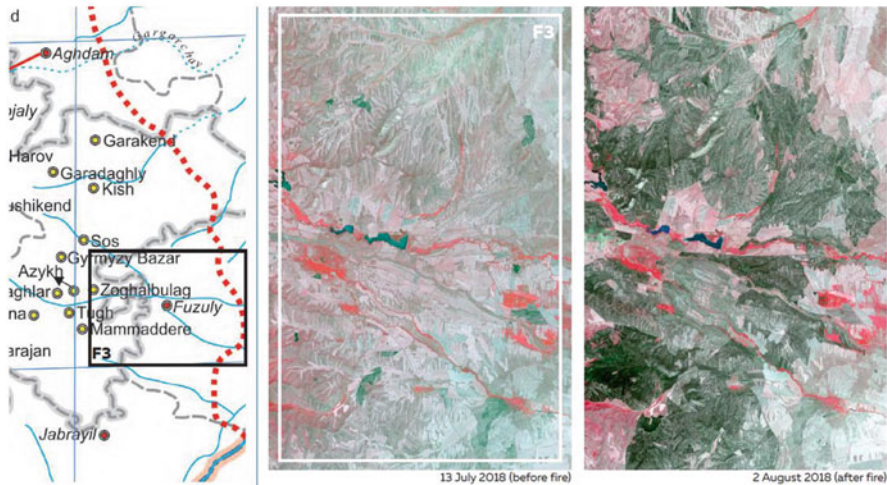


**Fig. 8** Expansion of tailing dump caused by exploitation of Demirli open-pit copper molybdenum mine near Demirli, Gulyatag, and Janyatag villages in the occupied part of the Tartar district ( $46^{\circ} 46' 16.713''$  E,  $40^{\circ} 9' 2.801''$  N)



**Fig. 9** Deforestation caused by mining activities near Chardagly village in the occupied part of the Tartar district ( $46^{\circ} 41' 33.965''$  E,  $40^{\circ} 14' 9.393''$  N)

- Hydroelectric power plant in the west of the Sarsang Water Reservoir in the occupied part of the Tartar district ( $46^{\circ} 32' 0.862''$  E,  $40^{\circ} 8' 38.201''$  N)
- Control point on the Goris (Armenia)–Khankandi road near Zabukh village in the occupied Lachyn district ( $39^{\circ} 35' 36''$  N,  $46^{\circ} 32' 10''$  E)



**Fig. 10** Burned area covering 347 km<sup>2</sup> and affecting 25 villages in the occupied Fuzuli district stretching 22 km from the South to the North and 17 km from the East to the West (39° 36' 24.92" N, 47° 06' 26.71" E)

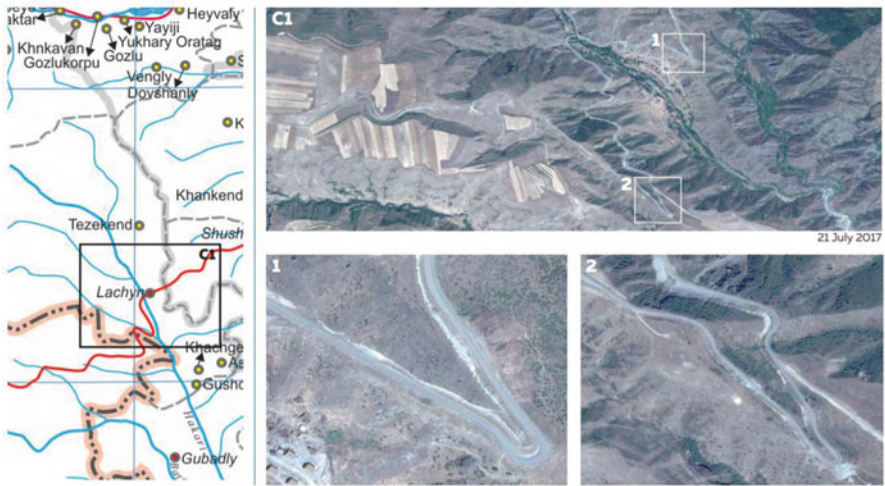
- Infrastructure in support of exploitation of copper-gold and molybdenum mine near Demirli village in the occupied part of the Tartar district (40° 08' 59" N, 46° 47' 12" E)
- Infrastructure in support of exploitation of Gyzybulag underground gold and copper mine near Heyvaly village in the occupied Kalbajardistrict (40° 08' 43" N, 46° 35' 50" E) (Figs. 11, 12, 13, 14, 15, and 16)

### Exploitation and Pillage of Natural Resources

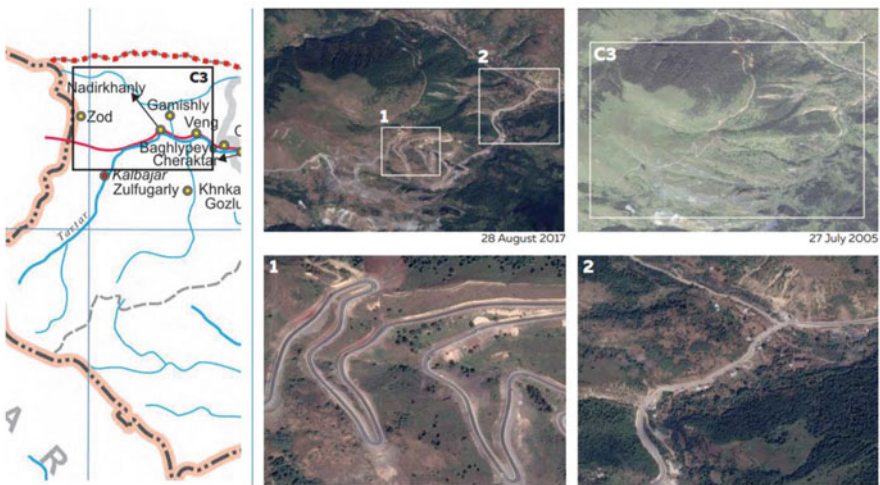
The environmental and economic damage, resulted by the high scale of exploitation and pillage of natural resources in the occupied territories of Azerbaijan, such as mining of minerals and metals utilizing heavy engineering machinery and equipment, is monitored and assessed by means of remote sensing techniques. (See Section XIII (Systematic pillaging, exploitation of and illicit trade in assets, natural resources and other forms of wealth in the occupied territories) of the Report of the Ministry of Foreign Affairs of the Republic of Azerbaijan (2016).)

The following examples of exploitation and pillage of natural resources are presented:

- Mining activities on 859.7 ha near Janyatag village in the occupied part of the Tartar district (40° 09' 08" N, 46° 46' 14" E)
- Mining activities on 44.78 ha near Chardagly village in the occupied part of the Tartar district (40° 14' 04" N, 46° 41' 49" E)



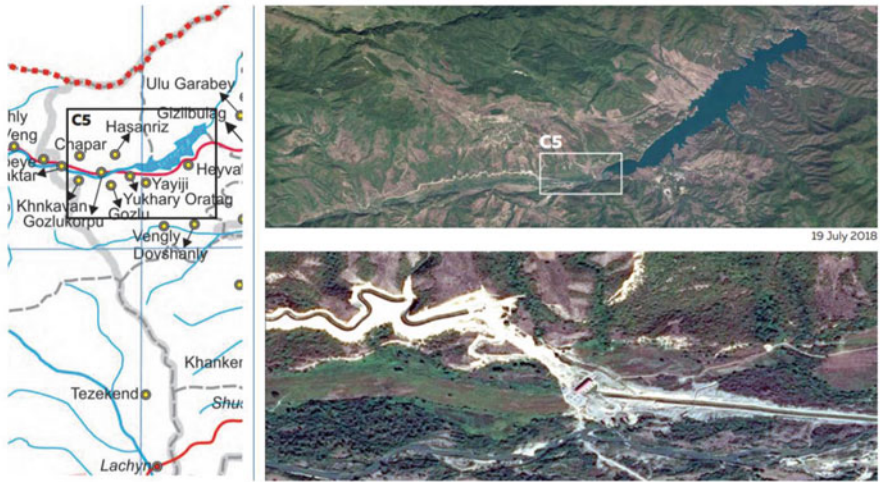
**Fig. 11** Reconstruction of Goris (Armenia)–Khankandi road passing through the occupied Lachyn district (39° 36' 17" N, 46° 32' 43" E)



**Fig. 12** Construction of Vardenis (Armenia)–Aghdara highway passing through the occupied Kalbajar district (40° 13' 18" N, 45° 58' 59" E)

- Mining and ore processing facilities on 63.78 ha of the Gyzybulag underground mine near Heyvaly village in the occupied Kalbajar district (40° 08' 29" N, 46° 35' 38" E)
- Mining activities in the Tutkhum gold-molybdenum deposit in the occupied Kalbajar district (40° 01' 14" N, 46° 09' 36" E)



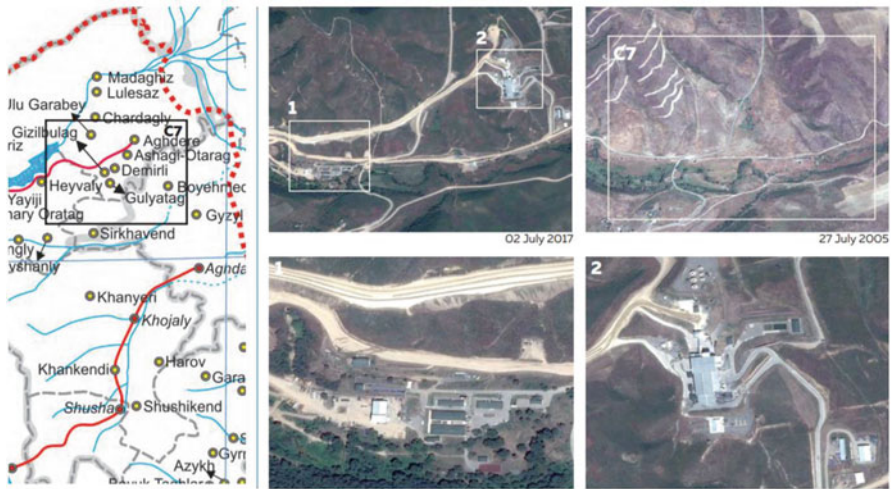


**Fig. 13** Hydroelectric power plant in the west of the Sarsang Water Reservoir in the occupied part of the Tartar district (46° 32' 0.862" E, 40° 8' 38.201" N)

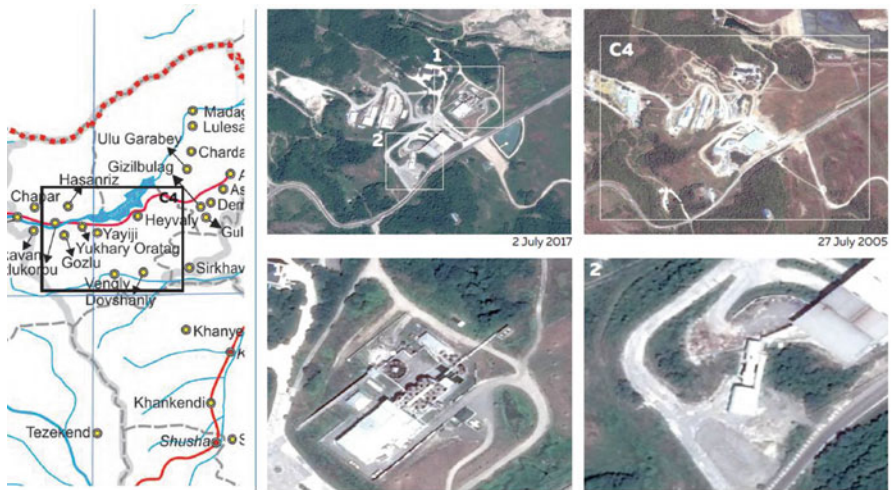


**Fig. 14** Control point on the Goris (Armenia)–Khankandi road near Zabukh village in the occupied Lachyn district (39° 35' 36" N, 46° 32' 10" E)

- Mining activities on 442.17 ha of Soyudlu gold mine in the occupied Kalbajar district (40° 14' 01" N, 45° 58' 17" E)
- Mining and ore processing facilities on 70.10 ha of gold mine near Vejnaly village of the occupied Zangilan district (38° 55' 52" N, 46° 31' 40" E) (Figs. 17, 18, 19, 20, 21, and 22)



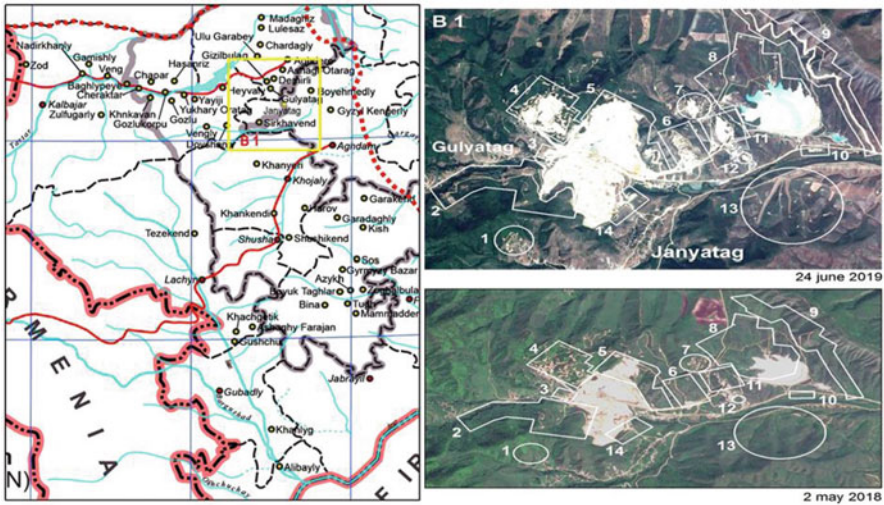
**Fig. 15** Infrastructure in support of exploitation of copper-gold and molybdenum mine near Demirli village in the occupied part of the Tartar district (40° 08' 59" N, 46° 47' 12" E)



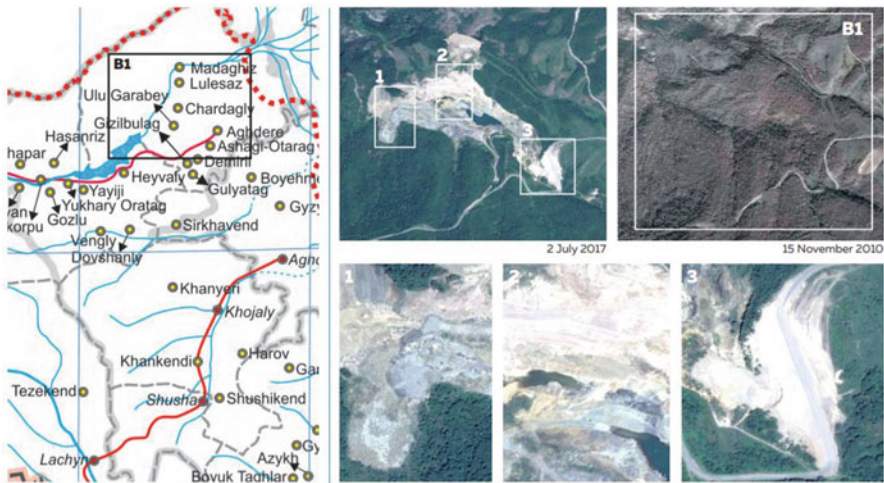
**Fig. 16** Infrastructure in support of exploitation of Gyzybulag underground gold and copper mine near Heyvaly village in the occupied Kalbajar district (40° 08' 43" N, 46° 35' 50" E)

**Destruction of Public and Private Property, Including Historical and Cultural Heritage**

Extensive destruction and appropriation of public and private property, deconstruction of houses and buildings for use as constructive materials, construction of new buildings on lands of Azerbaijani displaced people, and altering and destruction of

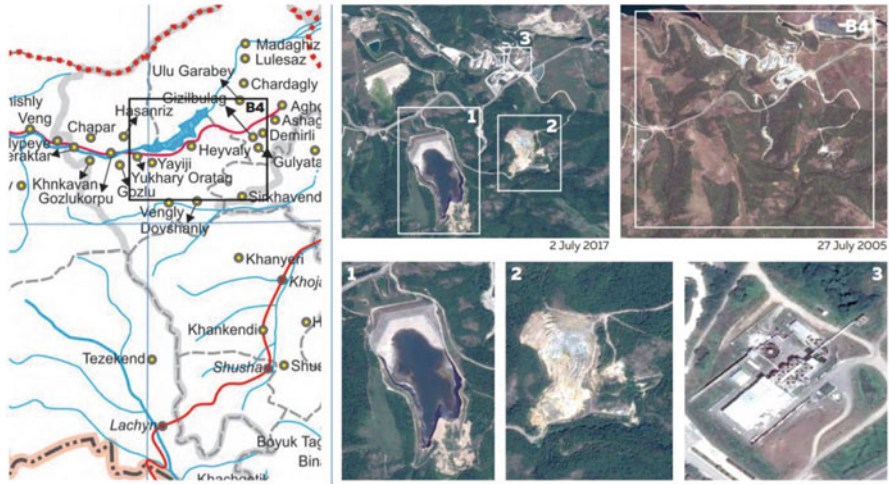


**Fig. 17** Mining activities on 859.7 ha near Janyatag village in the occupied part of the Tartar district (40° 09' 08" N, 46° 46' 14" E)

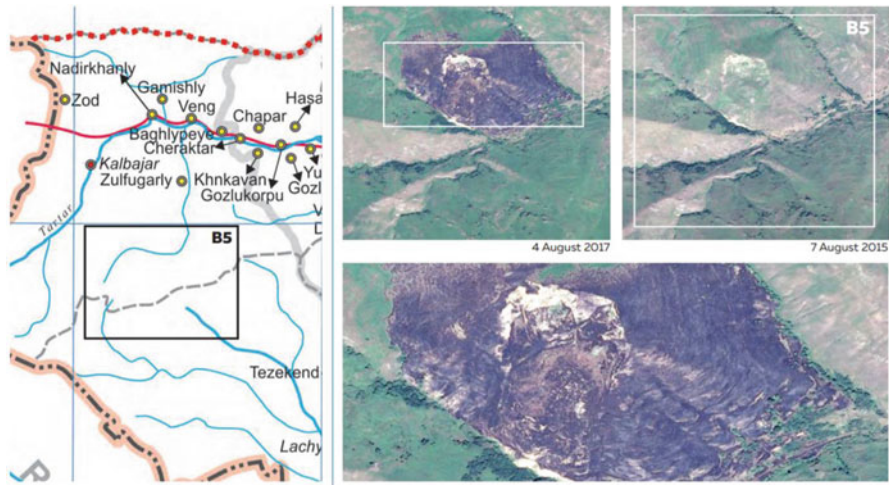


**Fig. 18** Mining activities on 44.78 ha near Chardagly village in the occupied part of the Tartar district (40° 14' 04" N, 46° 41' 49" E)

historical and cultural features, including the archeological, cultural, and religious monuments, are also the catastrophic results of the occupation of the territories. (See Section XIII (Systematic pillaging, exploitation of and illicit trade in assets, natural resources and other forms of wealth in the occupied territories) and Section XVI (Archaeological excavations, embezzlement of artefacts, altering of cultural



**Fig. 19** Mining and ore processing facilities on 63.78 ha of the Gyzybulag underground mine near Heyvaly village in the occupied Kalbajar district (40° 08' 29" N, 46° 35' 38" E)

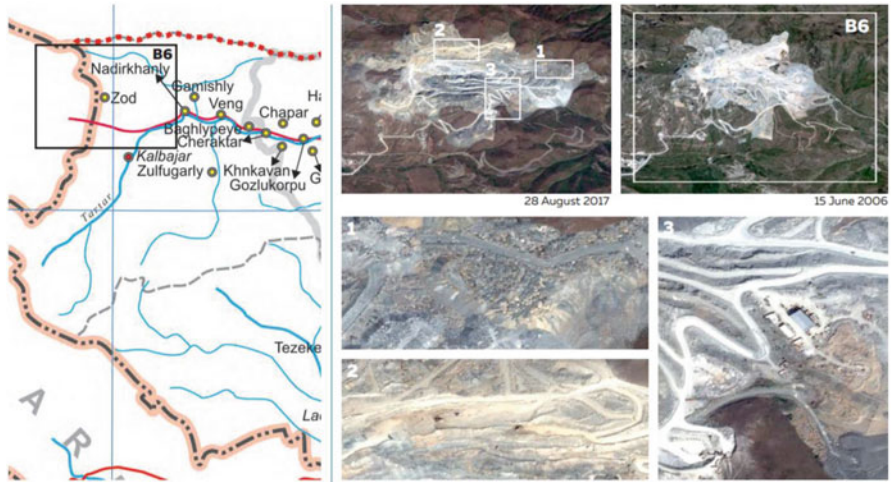


**Fig. 20** Mining activities in the Tutkhum gold-molybdenum deposit in the occupied Kalbajar district (40° 01' 14" N, 46° 09' 36" E)

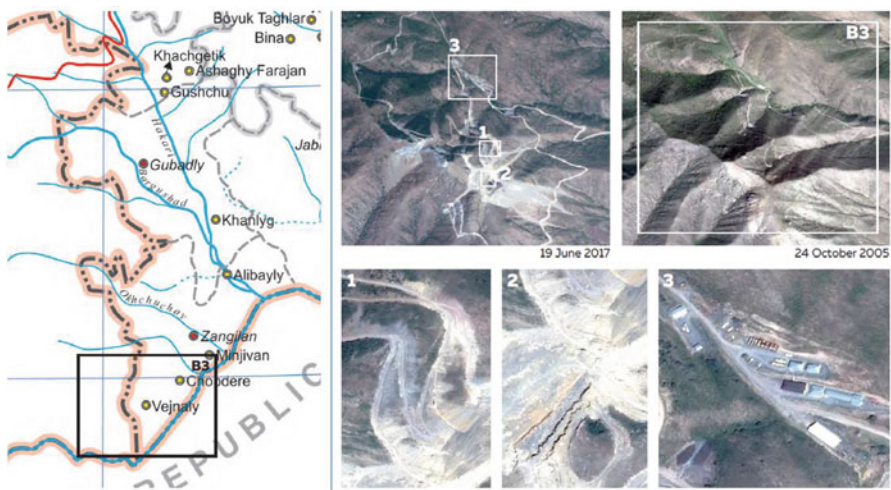
character of the occupied territories) of the Report of the Ministry of Foreign Affairs of the Republic of Azerbaijan (2016).)

The following examples of destruction of public and private property, including historical and cultural heritage, are presented:

- Destroyed town of Fuzuli of the occupied Fuzuli district (39° 35' 56" N, 47° 08' 49" E)



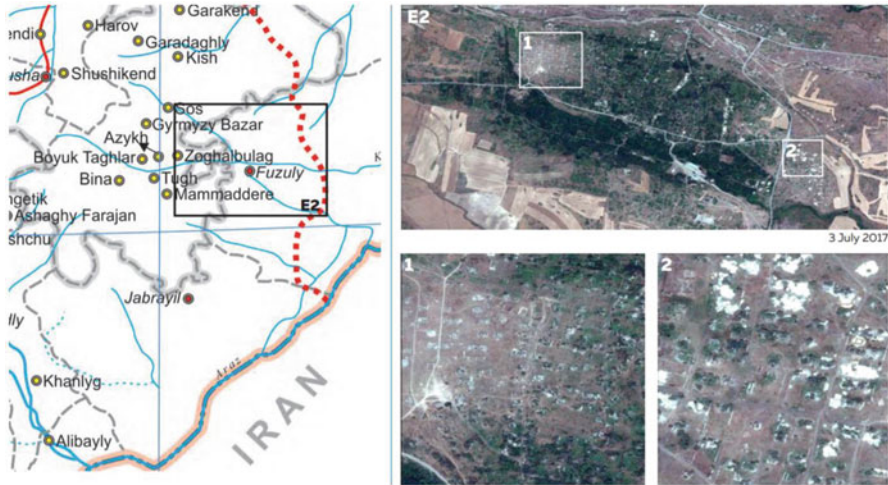
**Fig. 21** Mining activities on 442.17 hectares of Soyudlu gold mine in the occupied Kalbajar district (40° 14' 01" N, 45° 58' 17" E)



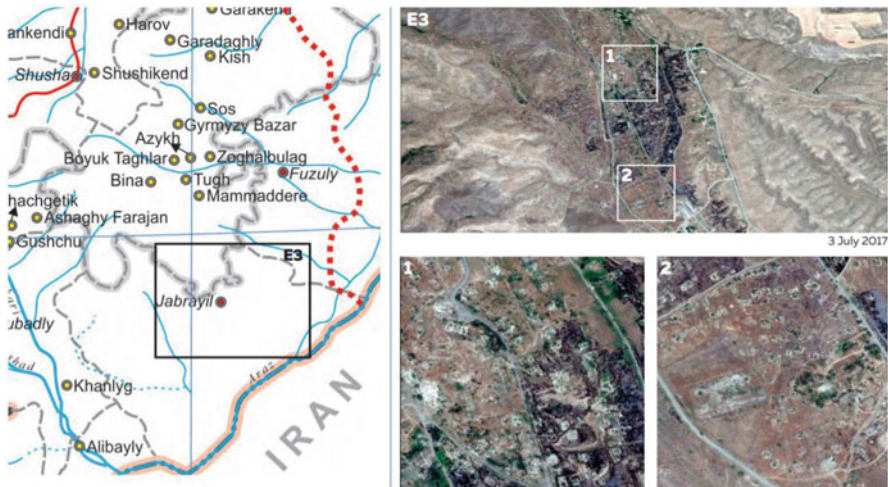
**Fig. 22** Mining and ore processing facilities on 70.10 ha of gold mine near Vejnaly village of the occupied Zangilan district (38° 55' 52" N, 46° 31' 40" E)

- Destroyed town of Jabrayil of the occupied Jabrayil district (39° 23' 56" N, 47° 01' 39" E)
- Severely damaged Saatly Mosque in the town of Shusha in the occupied Shusha district (39° 45' 45.26" N, 46° 45' 3.49" E)
- Destroyed Ashaghy Govhar Agha Mosque in the town of Shusha in the occupied Shusha district (39° 45' 42.31" N, 46° 45' 14.22" E)

- Destroyed Juma Mosque in the town of Aghdam in the occupied Aghdam district ( $39^{\circ} 59' 35.91''$  N,  $46^{\circ} 55' 53.88''$  E)
- Ruins of Ismailbayli village of the occupied Aghdam district ( $39^{\circ} 56' 02''$  N,  $47^{\circ} 00' 19''$  E) (Figs. 23, 24, 25, 26, 27, and 28)



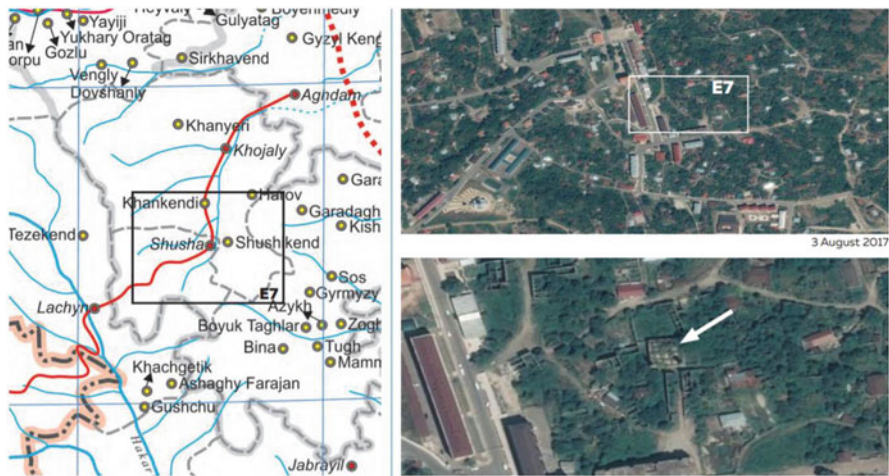
**Fig. 23** Destroyed town of Fuzuli of the occupied Fuzuli district ( $39^{\circ} 35' 56''$  N,  $47^{\circ} 08' 49''$  E)



**Fig. 24** Destroyed town of Jabrayil of the occupied Jabrayil district ( $39^{\circ} 23' 56''$  N,  $47^{\circ} 01' 39''$  E)



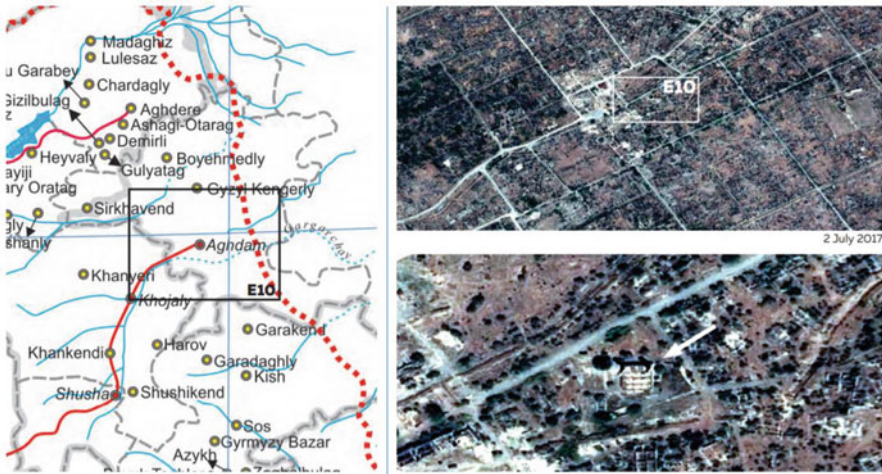
**Fig. 25** Severely damaged Saatly Mosque in the town of Shusha in the occupied Shusha district (39° 45' 45.26" N, 46° 45' 3.49" E)



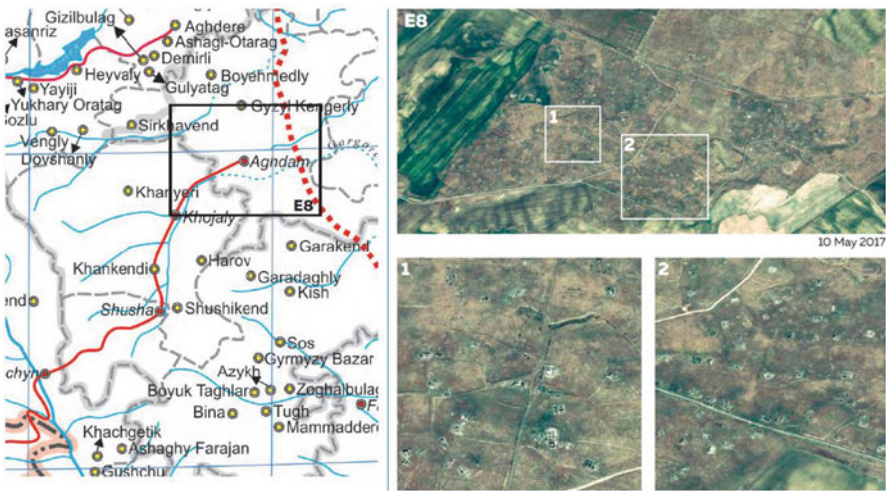
**Fig. 26** Destroyed Ashaghy Govhar Agha Mosque in the town of Shusha in the occupied Shusha district (39° 45' 42.31" N, 46° 45' 14.22" E)

### Exploitation of Agricultural and Water Resources

The settlements in the occupied territories rely primarily on agriculture development and water resources, which is pursued for economic and demographic reasons. Farmlands in Zangilan, Gubadly, Jabrayil, and other occupied districts, abandoned



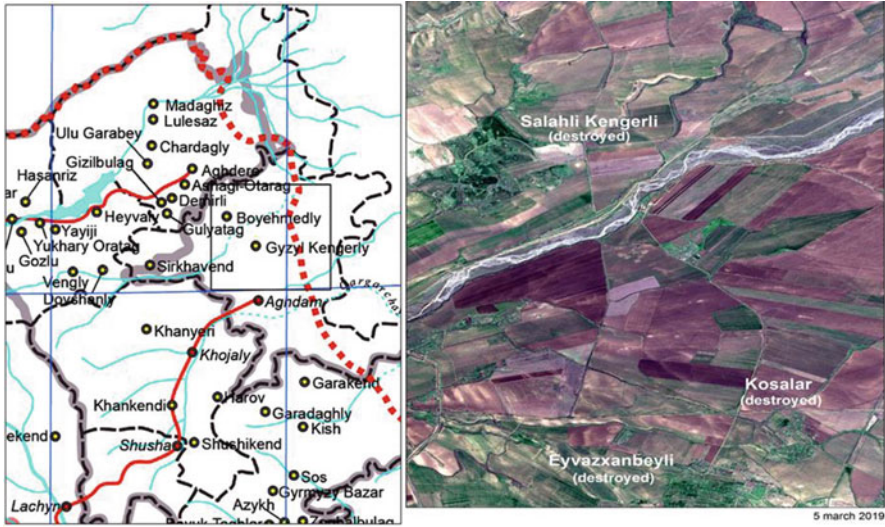
**Fig. 27** Destroyed Juma Mosque in the town of Aghdam in the occupied Aghdam district (39° 59' 35.91" N, 46° 55' 53.88" E)



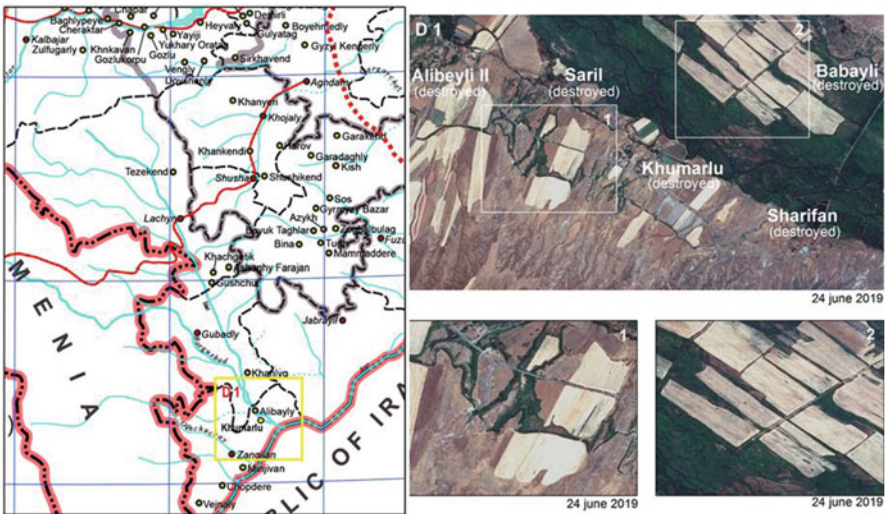
**Fig. 28** Ruins of Ismailbayli village of the occupied Aghdam district (39° 56' 02" N, 47° 00' 19" E)

by Azerbaijani people, have been extremely exploited. The waters of Araz River and other rivers are diverted, and the existing and new artesian wells, pump stations, and irrigation canals are serving the settlements and farming areas. (See Section XII (Extensive exploitation of agricultural and water resources) of the Report of the Ministry of Foreign Affairs of the Republic of Azerbaijan (2016).)





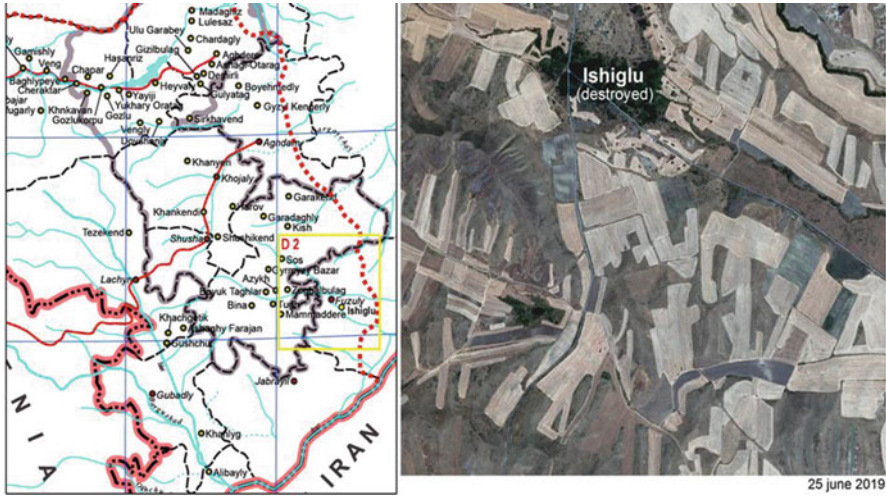
**Fig. 29** Agricultural activities near the Salahlı Kengerli village in the occupied Aghdam district (46° 56' 34.56" E, 40° 06' 49.37" N)



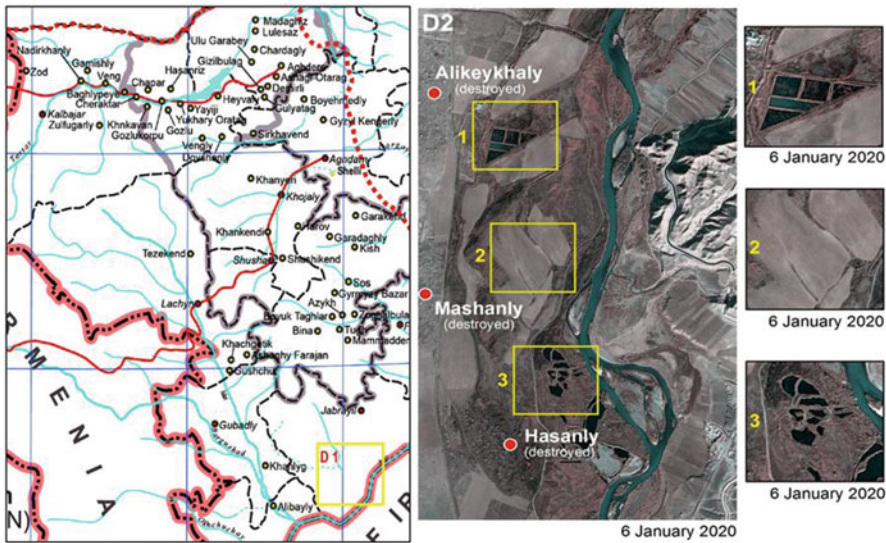
**Fig. 30** Agricultural activities near the Khumarlu village in the occupied Zangilan district (39° 08' 38" N, 46° 46' 45" E)

The following examples of exploitation of agricultural and water resources are presented:

- Agricultural activities near the Salahlı Kengerli village in the occupied Aghdam district (46° 56' 34.56" E, 40° 06' 49.37" N)

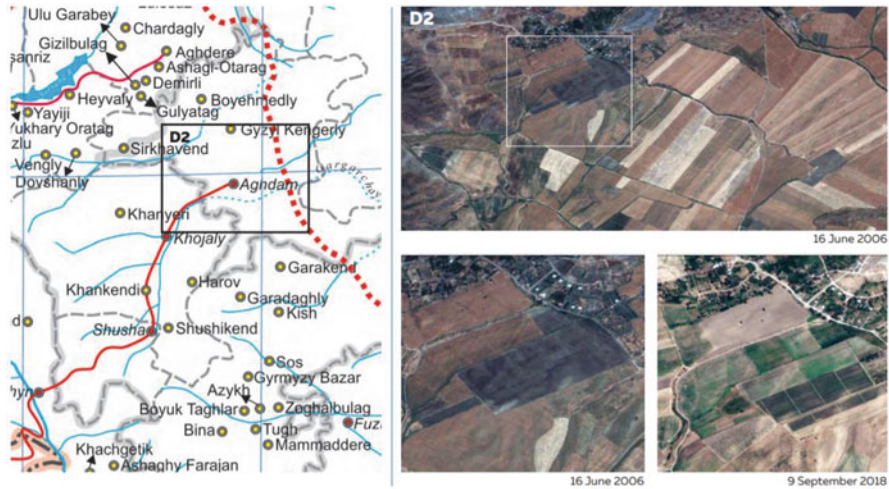


**Fig. 31** Agricultural activities near the Ishiglu village in the occupied Fizuli district (39° 08' 38" N, 46° 46' 45" E)

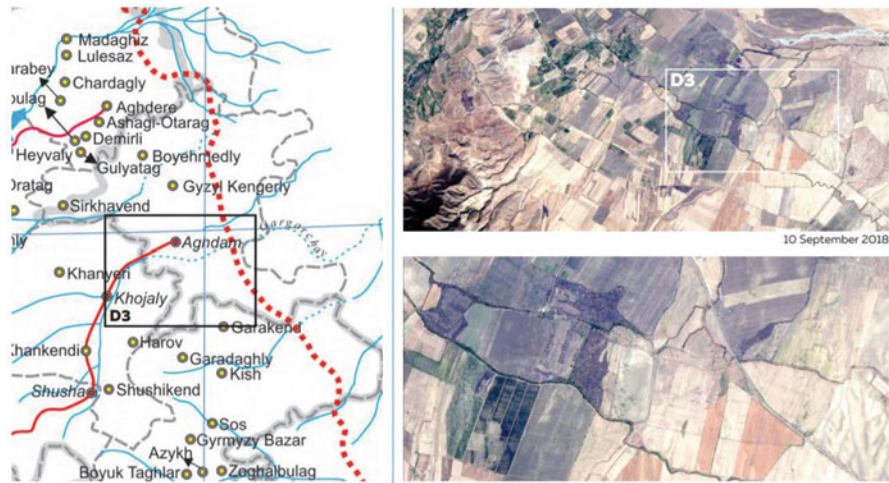


**Fig. 32** Agricultural activities near the Mashanly village in the occupied Jabrayil district (39° 13' 32" N, 47° 03' 04" E)

- Agricultural activities near the Khumarlu village in the occupied Zangilan district (39° 08' 38" N, 46° 46' 45" E)
- Agricultural activities near the Ishiglu village in the occupied Fizuli district (39° 08' 38" N, 46° 46' 45" E)

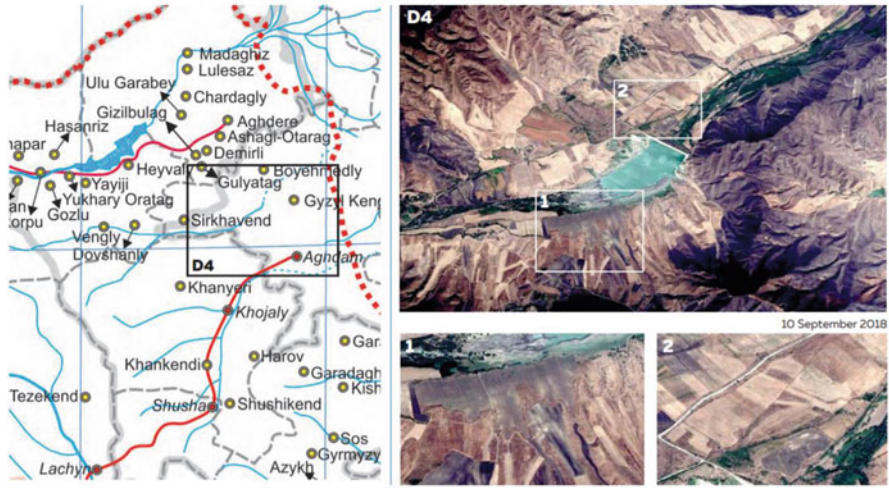


**Fig. 33** Newly sown agricultural lands in the southwest of Shelly village in the occupied part of the Aghdam district ( $46^{\circ} 53' 35.324''$  E,  $39^{\circ} 56' 58.337''$  N)

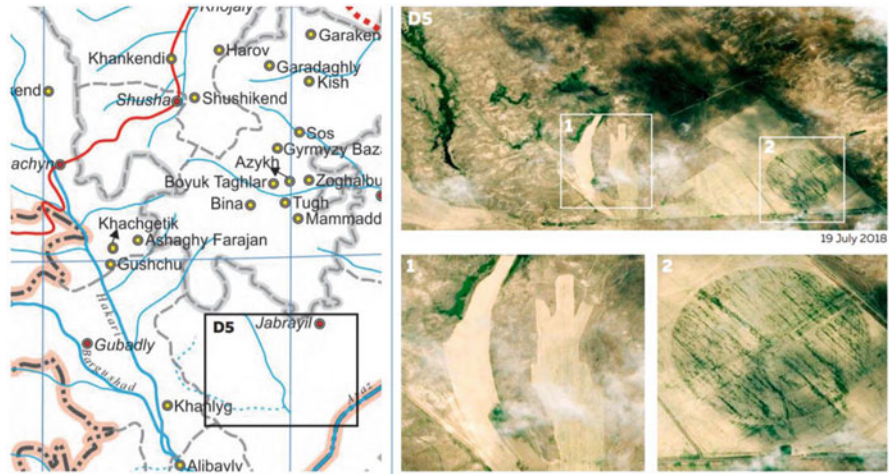


**Fig. 34** Newly sown agricultural areas near Shelly village in the occupied part of the Aghdam district ( $46^{\circ} 54' 46.658''$  E,  $39^{\circ} 57' 18.185''$  N)

- Agricultural activities near the Mashanly village in the occupied Jabrayil district ( $39^{\circ} 13' 32''$  N,  $47^{\circ} 03' 04''$  E)
- Newly sown agricultural lands in the southwest of Shelly village in the occupied part of the Aghdam district ( $46^{\circ} 53' 35.324''$  E,  $39^{\circ} 56' 58.337''$  N)
- Newly sown agricultural areas near Shelly village in the occupied part of the Aghdam district ( $46^{\circ} 54' 46.658''$  E,  $39^{\circ} 57' 18.185''$  N)

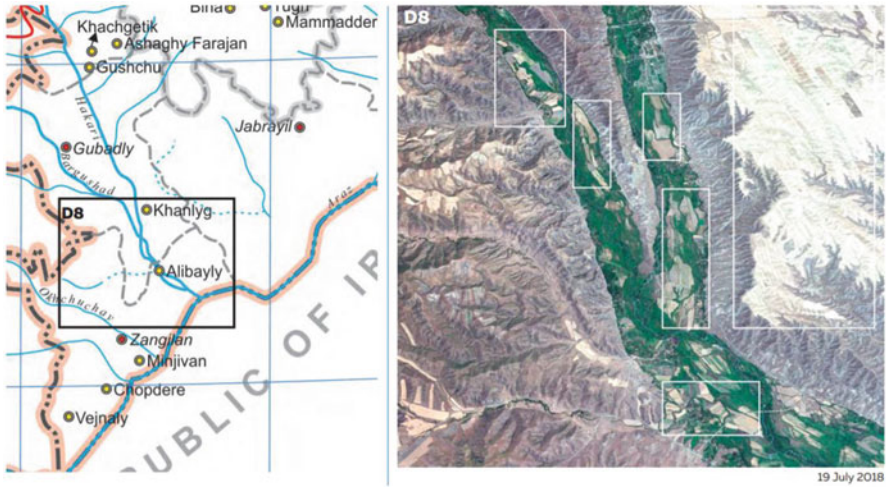


**Fig. 35** Exploitation of agricultural lands along the Khachinchay River near the Khachinchay Water Reservoir in the occupied part of the Aghdam district ( $46^{\circ} 49' 44.735''$  E,  $40^{\circ} 2' 45.579''$  N)

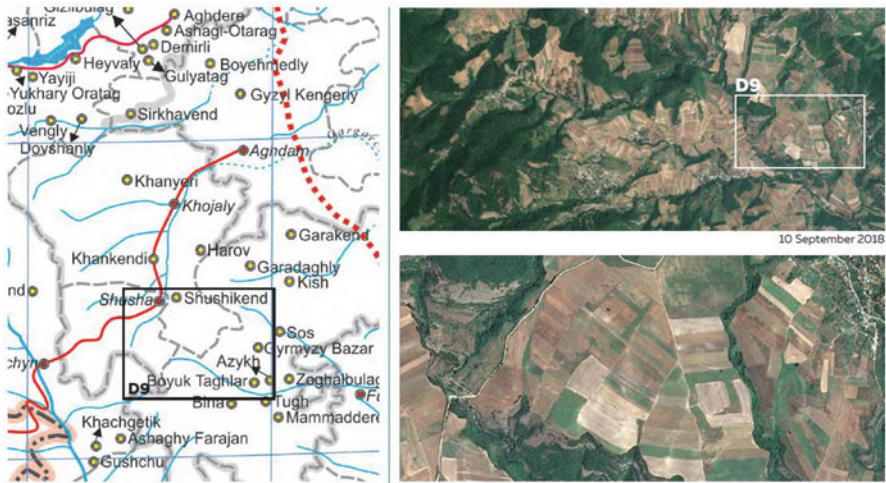


**Fig. 36** Exploitation of agricultural lands along the Araz River in the occupied Jabrayil district ( $47^{\circ} 2' 8.634''$  E,  $39^{\circ} 15' 52.574''$  N)

- Exploitation of agricultural lands along the Khachinchay River near the Khachinchay Water Reservoir in the occupied part of the Aghdam district ( $46^{\circ} 49' 44.735''$  E,  $40^{\circ} 2' 45.579''$  N)
- Exploitation of agricultural lands along the Araz River in the occupied Jabrayil district ( $47^{\circ} 2' 8.634''$  E,  $39^{\circ} 15' 52.574''$  N)



**Fig. 37** Exploitation of agricultural lands along the Hakari River in the occupied Zangilan and Gubadly districts (39° 36' 17" N, 46° 32' 43" E)



**Fig. 38** Exploitation of agricultural lands near Chanagchi, Khanyeri, Khanabad, and Shushikend villages in the occupied Khojaly district (46°50'27.382"E, 39°43'54.474"N)

- Exploitation of agricultural lands along the Hakari River in the occupied Zangilan and Gubadly districts (39° 36' 17" N, 46° 32' 43" E)
- Exploitation of agricultural lands near Chanagchi, Khanyeri, Khanabad, and Shushikend villages in the occupied Khojaly district (46°50'27.382" E, 39°43'54.474" N) (Figs. 29, 30, 31, 32, 33, 34, 35, 36, 37, and 38)

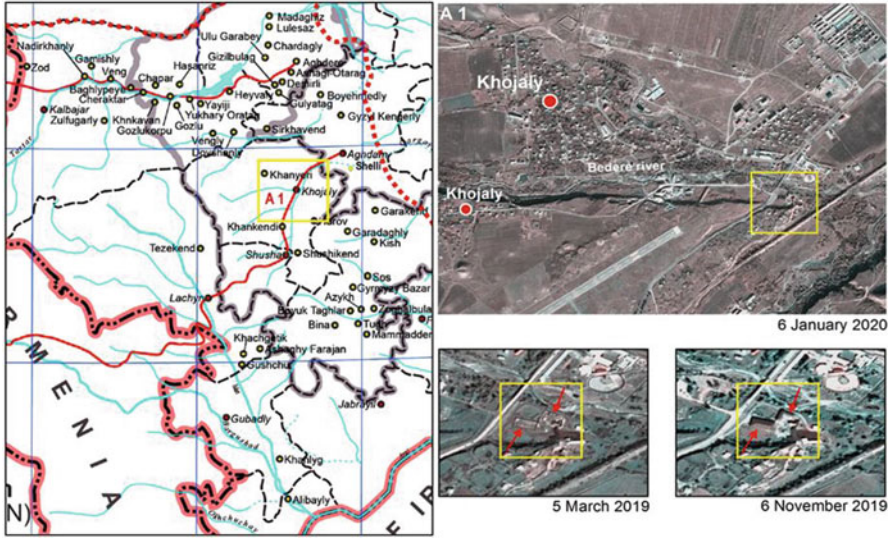


Fig. 39 Construction of new buildings in the occupied Khojaly city (39° 54' 29" N, 46° 48' 20" E)

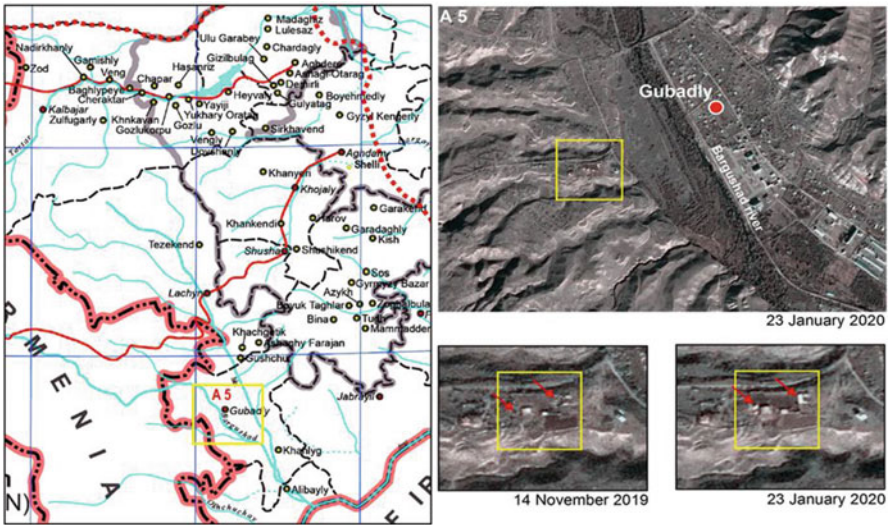
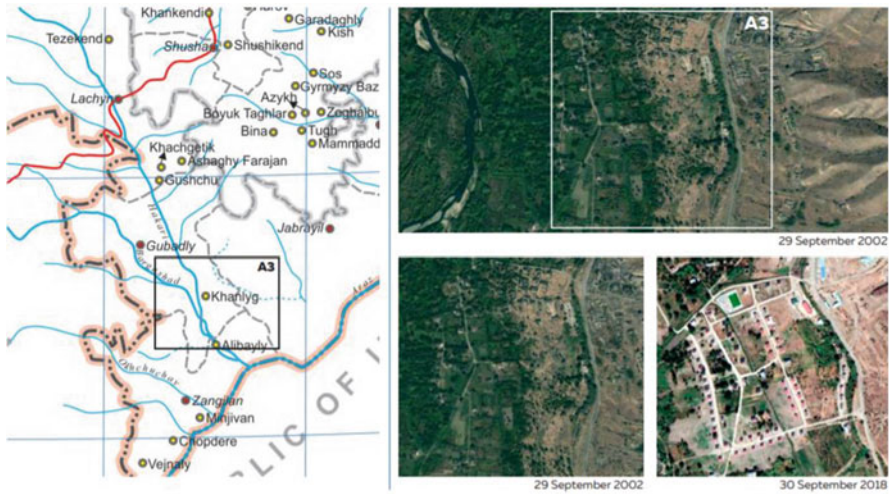


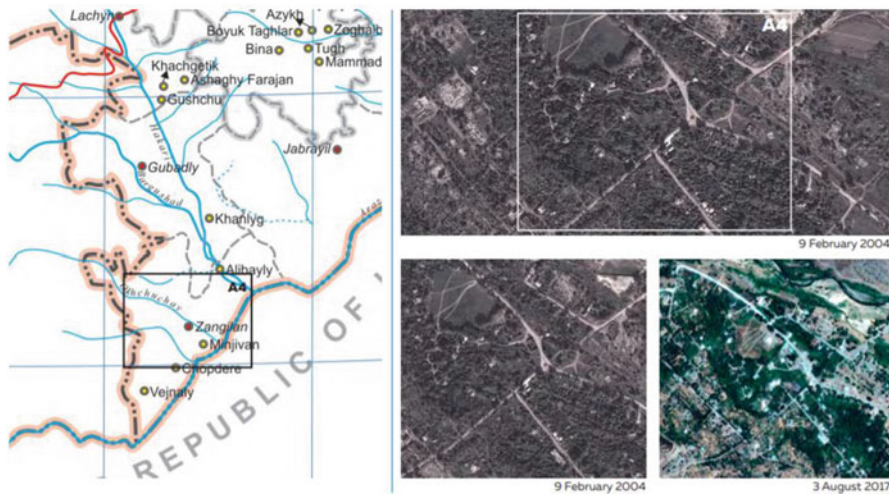
Fig. 40 Construction of new buildings in the occupied Gubadly city (39° 20' 30" N, 46° 34' 23" E)

### Implantation of Settlers and Construction of Permanent Social Infrastructure

The scale of construction and renovation of residential buildings and other associated social infrastructure has been critically increased, which is carried out for the



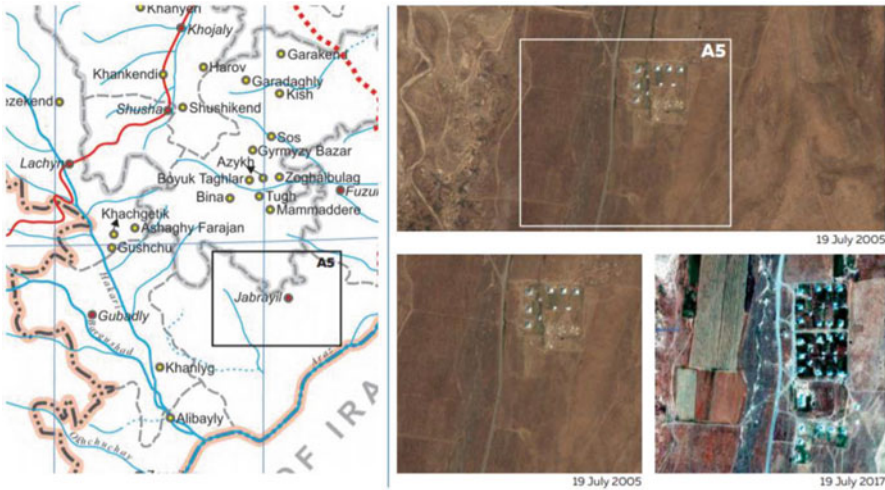
**Fig. 41** New settlement in Khanlyg village in the occupied Gubadly district (39° 16' 3.59" N, 46° 43' 13.12" E)



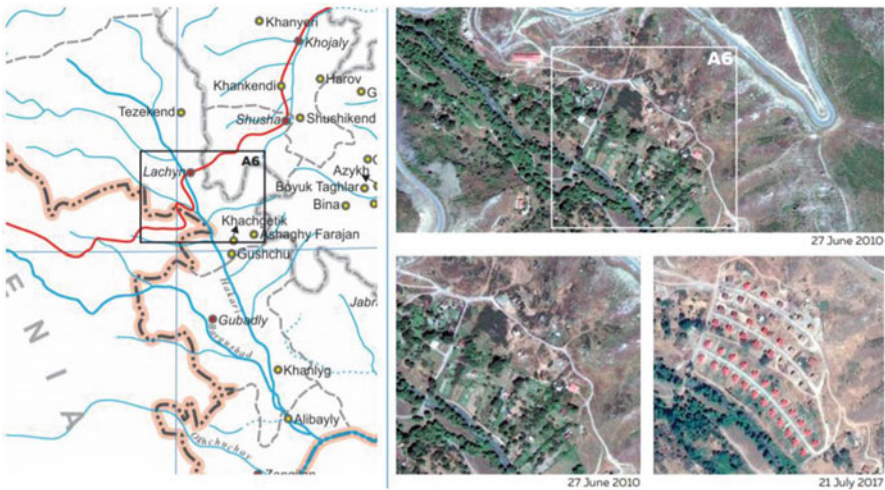
**Fig. 42** Newly built houses in the town of Zangilan in the occupied Zangilan district (39° 4' 55.67" N, 46° 39' 24.07" E)

support of continuous settlement activities. (For more details see Section VIII (Implantation of settlers from Armenia and abroad in the occupied territories) of the Report of the Ministry of Foreign Affairs of the Republic of Azerbaijan (2016).)

The following examples of implantation of settlers and construction of permanent social infrastructure in support of settlement activities are presented:



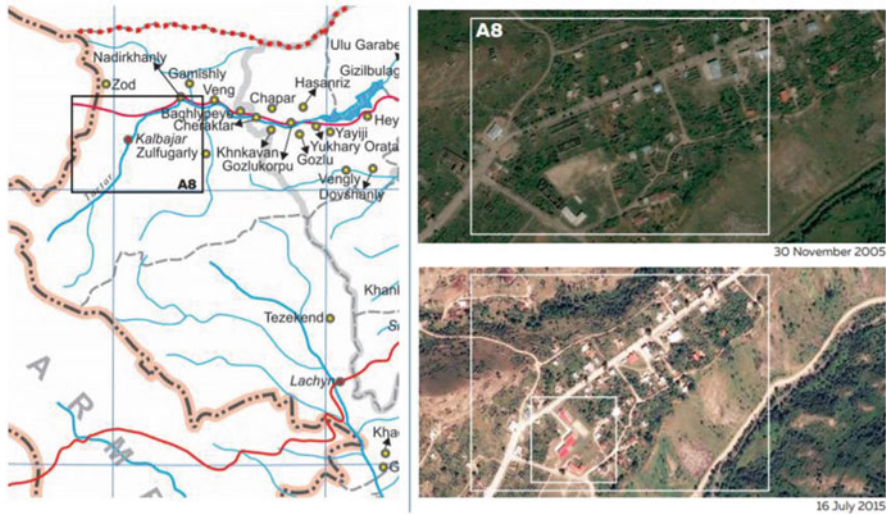
**Fig. 43** Newly established “Arajamugh” settlement in the occupied Jabrayil district (39° 21' 34.45" N, 47° 2' 3.54" E)



**Fig. 44** Newly established “Ariavan” settlement near Zabukh village in the occupied Lachyn district (39° 35' 27" N, 46° 32' 36.33" E)

- Construction of new buildings in the occupied Khojaly city (39° 54' 29" N, 46° 48' 20" E)
- Construction of new buildings in the occupied Gubadly city (39° 20' 30" N, 46° 34' 23" E)
- New settlement in Khanlyg village in the occupied Gubadly district (39° 16' 3.59" N, 46° 43' 13.12" E)





**Fig. 45** Newly constructed buildings in the town of Kalbajar in the occupied Kalbajar district (40° 6' 35.50" N, 46° 2' 42.07" E)

- Newly built houses in the town of Zangilan in the occupied Zangilan district (39° 4' 55.67" N, 46° 39' 24.07" E)
- Newly established “Arajamugh” settlement in the occupied Jabrayil district (39° 21'34.45" N, 47° 2' 3.54" E)
- Newly established “Ariavan” settlement near Zabukh village in the occupied Lachyn district (39° 35' 27" N, 46° 32' 36.33" E)
- Newly constructed buildings in the town of Kalbajar in the occupied Kalbajar district (40° 6' 35.50" N, 46° 2' 42.07" E)
- Newly constructed buildings in the town of Kalbajar in the occupied Kalbajar district (40° 6' 35.50" N, 46° 2' 42.07" E) (Figs. 39, 40, 41, 42, 43, 44, 45)

## Conclusion

Remote sensing by means of satellites is one of the main sources of data for military strategic planning and intelligence. Azerbaijan owns a high-resolution Earth observation satellite Azersky, which is used to continuously monitor the occupied territories, which constitute 20% of its territories, including the Nagorno-Karabakh region, the seven adjacent districts, and some exclaves.

The Azersky satellite in constellation with SPOT 6 is orbiting over the occupied territories of Azerbaijan, providing high-resolution images of specific zones of interest. The satellite imagery, acquired by Azercosmos, has provided the evidence of illegal activities on the occupied territories from Space, such as environmental damage, permanent infrastructure changes, exploitation and pillage of natural

resources, destruction of public and private property, implantation of settlers, and construction of permanent social infrastructure.

Despite the resolutions, adopted by UN Security Council, which reaffirmed that the Nagorno-Karabakh region is part of Azerbaijan and called for immediate, complete, and unconditional withdrawal of the occupying forces from all occupied territories of Azerbaijan, the occupant continues its illegal activities on the occupied territory. Azerbaijan continuously monitors its territories, revealing and providing the evidence of violation of international law from Space. (Illegal Activities in the Territories of Azerbaijan under Armenia's Occupation: Evidence from Satellite, "Azercosmos" OJSCo & Ministry of Foreign Affairs of the Republic of Azerbaijan, 2019.)

---

## References

- Deer, P., 1995. Digital Change Detection Techniques in Remote Sensing. Technical Report, DSTO-TR-0169. Department of Defence, Australia, p. 52
- Euro consult Research Report: Satellite-Based Earth Observation. Market Prospects to 2021, October 2012.
- Hussain M, Chen D, Cheng A, Wei H, Stanley D (2013) Change detection from remotely sensed images: From pixel-based to object-based approaches. *ISPRS J. Photogramm. Remote Sens.* 80:91–106
- Van Persie, M., Noorbergen, H.H.S., Van Den Broek, A.C., Dekker, R.J., (2000). Use of Remote Sensing Imagery for Fast Generation of Military Maps and Simulator Databases, National Aerospace Laboratory NLR, NLR-TP-2000-397.

## Further Reading

- <http://www.osce.org/mg/76209?download=true>
- [http://mfa.gov.az/files/file/MFA\\_Report\\_on\\_the\\_occupied\\_territories\\_March\\_2016\\_1.pdf](http://mfa.gov.az/files/file/MFA_Report_on_the_occupied_territories_March_2016_1.pdf)
- <https://president.az/articles/30731>
- <https://spacenews.com/42840airbus-sells-in-orbit-spot-7-imaging-satellite-to-azerbaija2n/>

---

## **Part III**

# **Space Applications and Supporting Services for Security and Defense**



# Introduction to Space Applications and Supporting Services for Security and Defense

# 37

Maarten Adriaensen

## Contents

Focus Areas .....	701
Conclusions .....	703

## Abstract

This introductory chapter to the Space Applications and Supporting Services for Security and Defense provides the overview of subjects and areas covered in the Part 3. Apart from the introductory chapter, 20 contributions cover a wide spectrum of space-based and space-enabled services and applications. The section aims to cover all main applications areas in generic chapters as well as to provide information about niche areas in specific chapters. Together, the identified and covered themes and issues provide a comprehensive setting of space-based and space-enabled services and applications for security and defense.

## Focus Areas

The security and defense interest in space came initially from the motivation to demonstrate ballistic missile capacities in the frame of nuclear deterrence. Subsequently, the operational use of space emerged considering the limitations of the ground and airborne assets used so far and the increasing added value from space-based services for Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR). In that frame, space enables services in

---

M. Adriaensen (✉)  
European Space Agency (ESA), Paris, France  
e-mail: [maarten.adriaensen@esa.int](mailto:maarten.adriaensen@esa.int); [maarten.cm.adriaensen@gmail.com](mailto:maarten.cm.adriaensen@gmail.com)

the fields of Satellite Remote Sensing (Earth Observation), Positioning, Navigation and Timing (PNT), Satellite Communications and Space Situational Awareness (SSA).

Numerous space operational applications routinely deliver indispensable fast and reliable services for security and defense. In terms of applications and services, space is indeed essentially the main global way of collecting, transmitting, and distributing information. Space-based services make a decisive contribution to the ability to conduct an effective foreign and security policy and to achieve whole-of-government security preparedness including defense aspects in a holistic approach. The relative dependency on space-based services in combination with the vulnerability of space assets drives countries to develop ways of protecting their critical space infrastructure, both civil and defense.

Satellite remote sensing information, based on the exploitation of imagery data derived from several category of sensors, electro-optical, radar, infrared (IR), multispectral, or laser, has important use in the security and defense domains. Earth Observation is an essential capability contributing to the intelligence picture at strategic, operational, and tactical levels and constitutes therefore a pivotal source of information for effective decision-making. A dedicated chapter on the role of satellite imagery in the frame of disaster management is included (H. de Boissezon and A. Eddy), as well as a chapter on Earth observation applications for security and defense purposes (F. Dolce, D. Di Domizio, D. Bruckert, A. Rodriguez, and A. Patrono). Complementing the chapters on specific remote sensing applications, a contribution on the regulatory aspects of remote sensing data completes the contributions on Earth Observation in this section of the Handbook (P. De Man).

Communication satellites are indispensable in support of command and control functions and are heavily used in military operations, requiring unique requirements for protected communications. The security operations also require such reliable communication services but without the same level of protection and thus rely on both commercial services and governmental satellites. The interpenetration of the military and civilian space communication services, however, increases with, on the one hand, the needs to connect mobile assets such as unmanned aircraft and network ground forces requiring large bandwidth and, on the other hand, the growth of the commercial market, driven by the demand for broadband Internet services and video distribution. A dedicated chapter on Satcom for security and defense is included in this section (H. Lueschow and R. Pelaez).

Positioning, Navigation and Timings (PNT) services and applications are crucial for security and defense purposes. GPS revolutionized military applications by providing accurate position, velocity, and time/synchronization information for all military assets worldwide, in all weather conditions, with a common time and geodetic reference frame supporting the essential interoperability requirement. Two chapters on GNSS for Security and PNT for defense are included in this section of the handbook (J. Martin; and M. Dettratti and F. Dolce).

Space-based assets and services are facing multiple threats. A chapter on various threats to Space Systems provides a first overview of the threats faced by space-based assets and services, both encompassing the space, ground, and link segments (X. Pasco). Space services must be resilient to interference and must offer technical

and procedural means to quickly remedy any interference occurring in services. Space system operators need to be able to identify the location and type of the interference or jamming source in order to take immediate and appropriate action. Besides electronic attacks, which interfere with the transmission of radiofrequency signals, cyberattacks target the data itself and the systems using data and information. A cyberattack on space systems can result in data loss, widespread disruptions, and even permanent loss of a satellite. One dedicated chapter addresses the setup of a cybersecurity space operations center (S. Llopis Sanchez, R. Mazzolin, I. Kechagloul, D. Wiemer, and J. Muylaert).

In the domain of SST and SSA, multiple chapters have been included in this section, considering the increasing global importance of SST and SSA, reflected in multiple programs developed in the USA, Europe, and other parts of the world. One chapter is dedicated to space object and event behavior quantification and assessment (M. Jah). Another chapter elaborates on STM through environment capacity from a holistic perspective (S. Lemmens). A specific chapter addresses the role of Artificial Intelligence in the frame of future SSA and STM (M. Vassile, L. Sanchez Fernandez-Mellado, and E. Minisci). The chapter on SST developments in Europe sheds a light on current development in the field of space surveillance capabilities in Europe (R. Peldszus and P. Faucher). Furthermore, this section includes a chapter on the status and evolution of space debris mitigation from a legal perspective (A. Nassisi, G. Guiso, M. Messina, and C. Valente). The risks to space-based services posed by space weather as well as the issue of Near-Earth Objects are addressed in this section with a specific chapter on space security in the context of cosmic hazards and planetary defense (J. Pelton) and a dedicated chapter on space weather services and applications (J. Janssens, J. Berghmans, P. Vanlommel, and J. Andries).

A dedicated chapter on space security and frequency management addresses the existing and upcoming challenges in that area (Y. Henri and A. Matas). The chapter on the use of space enabled services for food security focuses on the role of space assets and applications in the frame of agricultural post-harvest loss reduction in Africa (O. Adebola and S. Adebola). The chapter on a mega-constellation for space security provides a business case for commercial active debris removal (N. Veliev, A. Ivanov, and S. Biktimirov). Additionally, a specific chapter on security and defense applications from China features in this section (L. Shen, L. Hongbo, S. Zhang, and X. Wang). From the private sector perspective, a chapter is included on space security from the space operator perspective (J. Bureau).

---

## Conclusions

Space is increasingly competitive, congested, and contested. The chapters in this section III provide a very broad scope of the space security and defense interests in space-based and space-enabled services and applications. Throughout the generic and specific chapters in this section III, the objective is threefold:

- Providing a coherent and representative picture of the generic security and defense interests for space-based and space-enabled services and applications
- Introducing niche areas through specific contributions that complement the generic overviews for various space subdomains (including Earth Observation, PNT, Satcom, SSA) and cybersecurity, with attention for future developments as well as legal and business perspectives
- Reflecting the increasingly competitive, congested, and contested nature of Earth's orbital space from the services and applications viewpoint

**Disclaimer** The contents of this introduction and any contributions to the Handbook reflect my personal opinions and do not necessarily reflect the opinion of the European Space Agency (ESA).



# Earth Observation for Security and Defense **38**

Ferdinando Dolce, Davide Di Domizio, Denis Bruckert,  
Alvaro Rodríguez, and Andrea Patrono

## Contents

Introduction .....	706
Earth Observation Security and Defense Application Landscape .....	706
Earth Observation Missions and Applications for Security and Defense .....	710
Security and Defense EO Application .....	713
Examples of EO Operational Tasks and Services for Security and Defense .....	717
Examples of EO Operational Tasks .....	717
Copernicus SEA .....	719
Evolution of EO Services and Application at EU SatCen and Copernicus SEA .....	724
SatCen Service Evolution: Artificial Intelligence/Machine Learning .....	724
Copernicus SEA Service Evolution .....	726
Conclusion .....	728
References .....	729

## Abstract

The contents reported in this chapter reflect the opinions of the authors and do not necessarily reflect the opinions of the respective Agency/Institutions

Space-based Earth Observation is a consolidated capability providing added value to reach information superiority, a crucial enabler for operations in both security and defense domains. The availability and responsiveness of satellite payloads, together with exploitation capacity, allow to plan, monitor, and inform security and defense forces with performance not available with other means.

F. Dolce (✉) · D. Di Domizio  
European Defence Agency (EDA), Brussels, Belgium  
e-mail: [ferdinando.dolce@aeronautica.difesa.it](mailto:ferdinando.dolce@aeronautica.difesa.it); [davide.didomizio@eda.europa.eu](mailto:davide.didomizio@eda.europa.eu)

D. Bruckert · A. Rodríguez · A. Patrono  
EU Satellite Centre (EUSC), Madrid, Spain  
e-mail: [Denis.Bruckert@satcen.europa.eu](mailto:Denis.Bruckert@satcen.europa.eu); [Alvaro.Rodriguez@satcen.europa.eu](mailto:Alvaro.Rodriguez@satcen.europa.eu); [Andrea.Patrono@satcen.europa.eu](mailto:Andrea.Patrono@satcen.europa.eu)



This chapter describes how the gap between security and defense domains is increasingly blurred and the capacity to exploit the “big data” made available by the satellite systems and other contributing missions is becoming a common technological and operational challenge.

---

## Introduction

Space-based Earth Observation (SBEO) capabilities are one of the main data providers to imagery intelligence (IMINT) and geospatial intelligence (GEOINT) communities, since the technical and geographic information that can be derived from satellite systems through the interpretation or analysis of imagery is nowadays essential. However, SBEO products, including exploitation of imagery data derived from several categories of sensors, electro-optical, radar, infrared (IR), multi-spectral, or laser, can go well beyond IMINT/GEOINT domains and are used for both security and defense users for several purposes. Future SBEO satellites are providing big data from space and are building situation awareness, enabling the possibility to analyze the collected information, delivering products that will require strong optimization and improving in terms of delays in processing, interpreting, and disseminating to final customers. SBEO data/products, however, support also the monitoring phase, which relies on intelligence and is composed of two complementary functions: the early warning and the strategic surveillance. Furthermore, military planning, as well as geospatial support, also represents additional needs that can be accomplished through Space-based Earth Observation (SBEO) satellites’ data and products at both political, strategic, and operational level.

In recent years, there has been an increase in the development of tools and techniques to improve the exploitation of collected imagery data also to face the proliferation of SBEO assets. However, it is judged that the security and defense communities have not fully benefitted from this development, and they will need tools and procedures to fully take advantage of these technologies and to increase the trust in such kind of future supporting capabilities. One of the main difficulties will be the need to better balance and leverage the skills of analysts and operators within effective and efficient operational workflows and trusted data exploitation algorithms.

This chapter is mainly focused on the analysis of current and future applications to support security and defense missions using Space-based Earth Observation sources.

---

## Earth Observation Security and Defense Application Landscape

Earth Observation (EO) sensors mounted on space-borne platforms have now almost 50 years’ life – successful – story. Three systems which represent the founding pillars of EO commercial satellites era: (1) Landsat-1 (1972), the first EO satellite to

be launched to study and monitor the whole Earth's surface; (2) SPOT-1 (1986) that used a revolutionary commercial model for image distribution; (3) Ikonos (1999), the first commercial EO system capable to collect images with a ground sampling distance below 1 m (0.82 m) at Nadir (Denis et al. 2017). Meanwhile, US policy shift favored rapid market adoption for high-resolution satellite imagery anticipating a significant short- and long-term growth. Shortly after, DigitalGlobe launched QuickBird (2001).

In the last few years, there has been a proliferation of SBEO systems (archival, current, and planned – over 100 s of sensors (Committee on Earth Observation Satellites [www.ceos.org](http://www.ceos.org))) and others are now planned up to 2030 and beyond. Performance of sensors and mission technology has progressed over the last two decades. Overall, missions experimented longer endurance than expected and both optical and SAR sensors meliorated their design increasing, e.g., sensing performance, positional accuracy, and platforms' agility. Moreover, satellite systems progressively moved from the single-sensor model to the constellation approach. Performances have been boosted as well by the progressive implementation of the “dual-use” systems concept that allow different user communities to manage and exploit them taking advantage of a synergetic approach (despite configurations and rules may vary from mission to mission). The most recent development is the launch of nano- and micro-satellites (with constellations that can reach 100+). Lowering the cost of access to SBEO, they are becoming increasingly more attractive than conventional satellites. As an overall consequence, availability and access to data obtained by space-borne missions are increasing – and will continue to – in an exponential way, offering better and truly affordable observation capabilities at a greater range of spatial, spectral, and temporal resolutions (Belward and Skøien 2015; Denis et al. 2016; Toth and Józków 2016).

Image analysis production based and organized as a sequential series of human interventions in a pipe way may soon get overwhelmed in the new scenario shaped by huge observation data handiness and increasing computing capability. Providers sitting on massive amounts of exploitable data and user communities progressively expanding their analytical appetite for new products and services need faster and further interactive production modalities. The increasing development of web-based solutions and cloud-based services has allowed better quality of online functionality and performance without having necessarily to host and manage the data. Fast access to extensive archives of data, integration of diverse workflows user-specific, qualification of providers and users to work in diverse but interconnected environments to consume data, provide services, generate information and distribute products, are step by step leading the way of EO exploitation and derived value-added production. Any implementation can/shall be adapted for ad hoc security environments, without implying different design but with enforcement of specific security protocols and restrictions – no misuse or free outflow (Holmes et al. 2018). As an example, NGA (former) Director Robert Cardillo, during his keynote at the 2018 GEOINT Symposium in Tampa, announced a new online platform for open collaboration and development of geospatial solutions.

An important component of EO in supporting the primary aims of the space and security and defense domain is the provision of image and geospatial intelligence products and services resulting from the exploitation of remotely sensed data acquired by sensors mounted on space-borne assets. The reflections or emissions measured by the different types of sensors are depicted in images that need to be converted into meaningful information. Observation data are currently showing a new unique scenario in terms of variety, volume, velocity, veracity, and value. Geospatial information and EO, together with modern data processing and big data analytics, offer unprecedented opportunities (Lee and Kang 2015; Nativi et al. 2015; Câmara et al. 2016). There are different application approaches to face this challenge and they mainly depend on the type of sensor used and the sort of information that needs to be extracted.

Historically, in the security-defense environment, information is derived through a subjective analytical approach principally based on the experience and the skills of the analyst who visually interprets the image(s). The spatial and contextual way to proceed varies and depends on the objective of the study. Spatial, pattern, texture, and, in general, spectral information is most of the time improved by standard image processing technics (i.e., image enhancement) for increasing the visual distinction between features. Different collateral/ancillary data, spatially and temporally correlated with the imagery, made available through different sources, may complement the analytical process providing worthwhile information, essential in helping, confirming, etc. the interpretation course and its inferences (Campbell and Wynne 2011).

When the analysis needs to cover large areas, perform quantitative investigation, implement complex monitoring, rapidly highlight features not detectable at first view, (semi)automation of the analytical process may facilitate the interpretation process, e.g., decreasing the analysis time span and the risk of poor detection rates when compared to only human, lengthy, scrutiny approaches.

The application of robust algorithms/models to transform spectral into “meaningful” information offers an invaluable support. Nevertheless, deterministic models have to be accurately parameterized according to the sensor performance, the nature of the analyzed variables, and the information to infer for a specific task (Adams and Gillespie 2006). Since this approach needs an exhaustive knowledge, testing, and repeatable conditions to establish firm physical relations (that not necessarily exist and that ideally should be supported by an extensive fieldwork activity that most of the time – in the security-defense domain – is unfeasible for the nature of the requests and/or its location), alternative ways to proceed are used to facilitate the analytical process.

The statistical analysis of the spectral information and its supposed relationship with the phenomena to be assessed is used to reduce or transform the dimensionality of the data and to increase either the computational efficiency of, e.g., an image classification or the understating and manual extraction of the analyzed features (Lillesand et al. 2014).

Spectral rationing with adequately chosen spectral areas and appropriate wavebands or combinations of wavebands may as well facilitate the depiction of specific information. They can be used to better reflect the image content and, as

well, to further improve the performance of any of the hereby mentioned methods, including image fusion such as pan-sharpening techniques (Ghassemian 2016).

As temporal resolution of EO systems and constellations increased, multi-temporal data merging and change detection computing capacities augmented as well in terms of applicability and efficiency in supporting (semi)automatic monitoring of surface changes over varying time span intervals – including detection, estimation, and/or comparison of trends and dynamics (Fulcher et al. 2013; Hussain et al. 2013; Bovolo and Bruzzone 2015). This also simplifies the handling of the increasing load of imagery data, the controlling of alarms, and a better management of direct human involvement.

Where subjective, deterministic or statistical classic analysis become insufficient to identify relationships between the different pieces of available information – or simply are unknown or too lengthy, approximate, etc. to be established. Artificial Intelligence (AI) methods are progressively demonstrating the potential to get information out faster with more thorough and complete analysis. In recent years, neural network applications increasingly demonstrated better capability to automatically discover relevant contextual features in remotely sensed images (Arel et al. 2010; Long et al. 2017; Maggiori et al. 2017). Data volume and computational capacity increased exponentially, boosting precisely the application of neural network computing to satellite image (when compared to studies performed in the 1990s such as (Hepner et al. 1990) or (Atkinson and Tatnall 1997)). However, one of the major problems associated with precise recognition and extraction of objects from remotely sensed data is still the time and cost of wide-ranging training of algorithms, requiring experienced analysts (Ball et al. 2017), particularly when tasks to be undertaken are context specific and imply constant tailoring and precise knowledge, background, etc. as in the security-defense domain.

Collateral information gathered from social media are both worthy in supporting imagery analysis, and progressively more complex to use (i.e., floods of data, abundant, rapid, and accessible implying fast and qualified reactivity to provide the required situational awareness of relevant information) (Li et al. 2017). AI is as well improving the speed and accuracy of identifying enlightening evidences, allowing analysts to expand capacity, create new analytic products, etc. Reliable information gleaning has definitely progressed thanks to AI; nevertheless, it is still *in fieri* and constant adaptation and tailoring is often necessary to build up and maintain a knowledge data base, requiring expert interpretation processes to cope with uncertainty and/or incomplete information extraction.

The choice of analytic approach depends on the available data, the degree of understanding of the processes under examination, and the possible relationship between the EO data inputs and the goal of the analysis. In the security-defense domain, when the rather heterogeneous portfolio of possible EO-based services is considered, there is no rigid predefined approach to tackle any specific task. Experience, to be read as knowledge, understanding, mastering, etc., is at the core of any study and will guide the analyst to choose and combine, in an optimized way, any of the above-mentioned approaches, according to the context and the data availability. While operational use of EO keeps growing, gaps and opportunities for further

development to tackle increasingly complex operational applications still exist and will always need adequate experienced human supervision throughout the entire analytical process.

---

## **Earth Observation Missions and Applications for Security and Defense**

Space-based Earth Observation is now able to satisfy the growing needs of both security and defense entities and private customers coming worldwide since space systems are now becoming more and more numerous. Nowadays, it is expected that almost an infinite amount of information will be available, creating a high level of common awareness, while just a few years ago the prediction of a future information age was providing a different outlook. As matter of fact, the US commercial approach, known as “new space,” is moving the market in the clear direction of an easier and cheaper access to space, reducing the life and dimensions of space missions and increasing the number of systems in orbit (Space Strategy for Europe – European Commission COM 2016). Governmental institutions and small countries can see micro-satellites’ capabilities as the only opportunity to reach an independent, confidential, and trusted space-based capability due to the lower cost in development and launch phases they are promising.

On the other hand, in addition to real information, there is a lot of misleading information that can become a threat in modern warfare scenarios. In the past, such kind of information was not considered a relevant threat since they were limited to few numbers of potential events, while today it represents one of the most challenging threats to face. Criminal organizations can express their soft power generating misleading information, e.g., in the cyber domain. From this prospective, space-based information and communication services can represent a reservoir in terms of reliability and trustiness of the information more than other alternate sources.

In this congested and competitive space environment, EO products can certainly be derived by different platforms and the integration of the information coming from several sensor classes will represent the new bottleneck. With the availability of big data coming from space, such a huge offer of space imageries could move the equilibrium from the space to the ground segment. If yesterday access to space was the real challenge, and possibility to get access to space capabilities was the key enabling factor, now this is not anymore the case: the challenge will be the capability to acquire, store, manage, process, and deliver reliable and timely information, to be extracted by all essential data. Military will continue to define SBEO requirements in terms of accuracy and spectrum band; however, data fusion and integrated products merging different EO data, Positioning Navigation and Timing (PNT), and communication capabilities will be the key to deliver effective recognized pictures for defense operations.

Even considering that, the Ministries of Defences (MoDs) cannot certainly rely on commercial application to accomplish their task, especially if the data are

provided by foreign companies, that are able to exercise a shutter control in certain specific time and area of interest (AoI). It is then easy to understand that space institutional flagship programs turn to be strategic as they provide not only a full set of information but also the control of the data acquisition, flow, policy, and security.

Space-based data moreover solve a key issue in terms of autonomy to the MoDs. In fact, one of the biggest strengths of the SBEO systems is that they are not affected by sovereign rights of States “overflown” by spacecrafts (United Nations Treaties and Principles on Outer Space 2002). This makes possible to obtain information about the area of interest through means regulated by agreed international laws, without any engagement of the States overflown by the spacecraft.

Even if the difference between defense and security domains is not easy to identify and both concepts could lead to misinterpretation, it could be summarized as the following: security’s main task has to face with Member State’s internal risks without a prerecognized enemy or attack to face, e.g., terrorism; on the other hand, defense’s main task has to face with Member State’s threats against an external identified enemy (Britz and Eriksson 2005; French white paper on Defence and National Security 2013). From this simple, but of course not exhaustive definition, it is clear that the capabilities required to deal with these two different scenarios are not necessarily equal. Nevertheless, the evolution of the global international scenario is generating boundaries that are quite often not clearly defined. The power’s global model, in fact, is evolving quite rapidly moving from a clear unipolar international system after the end of Cold War, when some distinguished authors declared “The End of History” (Fukuyama 1989) to a more global and fragmented multipolar model, where the symmetry of previous scenarios is not anymore applicable. This asymmetry is certainly reflected into military operations, coping with a hybrid warfare scenario and threats that cannot be easily identified. In such conditions, the evolution of guerrilla environments led to an unclear definition and delineation of geospatial limits. The time when the Greek arena’s competition model was applicable looks today as an ancient memory, while strategic models based on oriental philosophies, referring mainly to Sun Tzu’s doctrine (Tzu 2007) where the art of camouflage is a key capability, are becoming more applicable to modern terroristic threats.

As a direct consequence of these new scenarios, the boundaries between internal and external activities are clearly not well identified, calling for an increasing application of defense capabilities for homeland security. Defense techniques, procedures, and expertise are now finding a great demand in the civilian and the security world (European External Action Service 2016).

Nevertheless, there are still specific tasks related to defense domain that mainly stick with military operations and this is true also in the case of SBEO applications. In EU dimension, the taxonomy developed in the framework of the European Defence Agency, the “Generic Military Task List” (GMTL) clearly define some tasks that are not applicable to security dimensions. The GMTL, for example, refers to the conduct and synchronization of joint precision strike aimed to conduct efficient application of joint precision firepower. For such kind of tasks, SBEO data and products can play a key role. High-accurate weapons, in fact, are based

on such kind of information that, if properly elaborated and ingested in the weapon system, produce a high added value. With the increase of revisit time and with the decreasing of processing time, also battle damage assessment (BDA), a typical military task could be supported by SBEO capabilities on top of more tactical vehicles, and a potential link between automatic change detection algorithms and tactical operational commanders could produce effective information ([https://www.eda.europa.eu/what-we-do/activities/activities-search/persistent-surveillance-long-term-analysis-\(sultan\)](https://www.eda.europa.eu/what-we-do/activities/activities-search/persistent-surveillance-long-term-analysis-(sultan)) 2019).

Furthermore, military planning is underpinned by a continuous process of information collection, military assessment, and analysis. The strategic planning, in particular, relies on information to be collected in conditions where forces are not yet deployed and the “expeditionary” characteristic of satellite systems, able to reach faraway points on the planet in a few hours and in the next future will be able to provide near-real time information with global coverage, are fundamental. On the other hand, geospatial support is a key enabler also for the planning and execution of military and civilian missions and operations, training, and exercises, and it is based on imageries also coming from space domain, supporting, in this case, tactical functions. Nowadays, geospatial support is essential in everyday life and hence it is even more necessary in security and defense operations (EU Capability Development Plan 2018). SBEO data are the pillars and the first layer to build on further information and to derive multiple products for multidomain assessments and to provide effective tools for decision making and military or mission commanders.

In addition to these specific military missions, in the domain of SBEO, there are three fundamental general requirements driving and steering the development of military space systems: availability, confidentiality, and integrity.

Starting from the integrity requirement and keeping in mind the disinformation threats are world-scale threats; it can be stated that only with an independent, well-defined, and verified information source, it is possible to implement armament control, confidence-building, and treaty monitoring, in particular in a framework of a common defense and security policy. To achieve this goal, MoDs shall have a reliable information source to reach a common situational awareness; otherwise, it will be difficult to set up a room to agree on a common foreign policy and to deal with common threats as well as to verify information accuracy. The point is, how such kind of requirement can influence the developments of future space-based reconnaissance systems.

In addition, SBEO applications present governance, data security, service continuity, and business model criticalities. For instance, the use of open-source applications not only involves criticality about the services themselves, but also allows to the service provider to gather and store key information about uses and users. The confidentiality is a general key issue for the future of information technology and this is particularly true for defense users, as revealed by recent application cases such as the application able to collect military positions around the globe through the use of connected fitness trackers (Fitness tracking app Strava gives away location of secret US army bases 2019). The same problem can be applied to commercial SBEO providers, where even only the information about the area and time of interest could

represent an intelligence information, pointing out the importance of the confidentiality requirement. These issues have a direct impact in terms of SBEO needs for military missions. It raises the problem not only of the production and the availability of the information, but also the question of the control and the security of the data provided for the MoDs use. When imagery is obtained through commercial companies directly contracted by local MoD, the integrity of the information could not be guaranteed. Technically speaking, imagery data can be manipulated, even if such kind of theoretical operations could require some delay in providing the requested service. By building up its own fleet of satellites or strong restricted commercial licenses, including ground segments and processing, these potential concerns are not in place anymore.

Finally, also based on recent military operations' experience, where a coalition of States is involved, the same data might be needed by all of them at the same time, implying the requirements of the availability of the data. For this kind of issue, data exchange agreements must be addressed accordingly, leading in some cases to considerable additional costs and delays, while a broader and structured pooling and sharing approach would probably lead to more effective benefits for the coalition.

---

## Security and Defense EO Application

Earth Observation from space in the defense sector was largely used historically for intelligence purposes, being considered as an extension of the capacity of spy aircrafts. In particular, the branch of intelligence dealing with imagery is known as IMINT.

IMINT is the technical, geographic, and intelligence information derived through the interpretation or analysis of imagery and collateral materials. It includes exploitation of imagery data derived from several categories of sensors: electro-optical, radar, infrared (IR), multispectral, or laser (US Joint Publication 2013).

The use of SBEO systems was initially devoted to specific strategic tasks (e.g., nuclear sites discovery). The current improvement of sensors' performance, the agility of the satellite platforms, and the possibility to integrate different datasets are important enablers allowing the use of SBEO also for more specific and repetitive tasks, even in direct support to missions and operations.

In this regard, system design parameters may however impose constraints on the ability to use SBEO satellites in military operations. The architecture of the mission and the choice of the orbit is one example of these constraints.

Traditionally, SBEO missions have been conceived with the use of low Earth sun-synchronous orbits. In this case, the complexity of system design was manageable thanks to the advantages of orbit stability, global coverage, constant sunlight on the platform, and of advantageous geometries for imagery collection. This type of orbit however limits the capacity of continuous observation (e.g., areas at equatorial latitudes are visited only twice a day), and moreover the satellite passes on target locations always at the same local time, reducing the possibility of discretionary



imaging. Constellations including several satellites, although improving the performance of continuous observation, would hardly be considered as sole source of information in the case of military operations.

Indeed, IMINT can be collected via satellites, but also with other assets: unmanned aerial vehicles, reconnaissance aircraft, and ground systems. These assets are not interchangeable and should be used in combination. A recent study conducted by the European Defence Agency evaluated the potential options to enhance collection capabilities in the area of IMINT through innovative and technologically feasible solutions, to meet the need of persistent surveillance of wide areas in defense and security operations ([https://www.eda.europa.eu/what-we-do/activities/activities-search/persistent-surveillance-long-term-analysis-\(sultan\)2019](https://www.eda.europa.eu/what-we-do/activities/activities-search/persistent-surveillance-long-term-analysis-(sultan)2019)). To this extent, the analysis based on operational scenarios provided the respective merits of assets/systems based on geostationary earth observation satellite systems, constellations of optical and radar small/mini satellites in low earth orbit, High Altitude Pseudo-Satellite Systems (HAPS), and Remotely Piloted Aircraft Systems (RPAS). The quantitative analysis performed, while showing that the performance in resolution of geostationary EO satellites seems yet to meet the requirements of military operations, demonstrated a real complementarity between the LEO constellations and other technologies which are likely to be used concurrently or successively in order to achieve the objectives pertaining to a given phase of operations.

The intelligence communities are used to develop their activities on the basis of the so-called intelligence cycle. The IMINT cycle mirrors the intelligence cycle. The steps in this cycle define a sequential, interdependent process for developing IMINT. The management of operations of SBEO systems used to produce IMINT is typically harmonized with the steps of the IMINT cycle: tasking, collection, processing, exploitation, and dissemination processes ([MCRP 2-10B.5 Imagery Intelligence – US Marine Corps](#)).

Concerning the exploitation of imagery information, imagery analysts have a central role in this domain, especially taking into account the traditional approach mostly built on visual interpretation of satellite imagery.

In the above described framework of big data environment, the traditional analysts' task of building situation awareness and producing actionable intelligence is changing and needs to be supported by modern tools to obtain the promising enormous added value coming from such numerous amounts of data. In several cases, current tools are not able to adequately support analysis, producing delays in the processing and in the interpretation or not allowing to take advantage of the real potential of big data.

In the defense domain, the use of modern technologies might be hampered by the need to comply with security rules, to work on "closed" classified systems to protect the data and the information, not relying on the support of distributed resources normally available in large private networks or on the Internet.

In the last years indeed, we witnessed a large development of tools and techniques reaching a good level of maturity in providing useful information by exploiting collected imagery data. However, the military operational communities have not benefitted in full of this technology growth. For instance, although new techniques

recently presented in the domain of big data analytics can provide added value for the security domain (Popescu et al.), a direct implementation in the defense applications needs to be properly addressed duly taking into account the still existing difficulties to put together the architectural elements of a cloud-based processing and the security constraints of classified systems. This does not mean however that defense imagery analysts are condemned to work with archaic tools.

As described previously, an important area of development is represented for instance by the future development of application of deep learning and artificial neural networks for imagery analysis. These capabilities will help to identify and refine the behavioral models by parsing and correlating the voluminous data streams available from space assets. Anomaly detection tools based on this concept are already available in Europe for the maritime domain with dual-use applications, valid both in defense (maritime situational awareness) and in security scenarios. Combining satellite radar imagery with Automatic Identification System (AIS) (IAC-14-B1.5.4 Cosmo-SkyMed data utilization and applications), Vessel Monitoring System (VMS), coastal radars, and any available intelligence data provide useful information to build a database of normal behaviors concerning the vessel tracks in specific area. Any deviation from recognized track patterns might be considered as an anomaly to be further investigated.

This is one practical example of the use of Synthetic Aperture Radar (SAR) satellite imagery. This technology has become a consolidated asset of military SBEO in Europe, thanks to important satellite programs (ref. COSMO-SkyMed, SAR-Lupe, COSMO-SkyMed Second Generation, SARah). The evolution from the first generation of the years 2000–2010 to the one under development in these years is making available considerably larger amounts of data, thanks to the improved resolutions, larger swaths, and more imagery per orbit.

In this case, the challenges deriving from the increased amount of data are complicated by the inherent complexity of SAR data and by the preponderance of historically well-established procedures that make use of electro-optical images to support military operations and the decision-making process, relegating in several cases SAR imagery to a secondary source of information.

On the contrary, a thorough exploitation of SAR imagery strengths would enlarge the use of SAR imagery alone and/or in combined use with electro-optical images, thus taking full advantage of its unique 24/7 and all-weather characteristics, therefore raising the effectiveness of investments made by several European Ministries of Defence on SAR satellites.

Ongoing studies are investigating new techniques aimed at developing solid procedures in support of SAR imagery analysts, overcoming the inherent difficulties of interpretation of “salt and pepper” images and with the objective to reach high automation levels ([https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-04-03-factsheet\\_react\\_2019](https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-04-03-factsheet_react_2019)).

The tasks can be performed by skilled analysts or by operators that might use tools developed for that purpose. In this regard, software exploitation tools for SAR images are available; however, the drawback is that those are not always able to extract and present the information that makes SAR images a product “easy and

ready to use.” In addition to this, the intrinsic peculiarities linked to the programming cycle of an SAR product and the lack of proper tools to assist the preparation of a task constitute an additional hurdle that limits the use of SAR images at operational level.

The procedures to analyses data are based on operational workflows. Those are defined as a series of activities that typically encompass several tasks: e.g., data preparation, data processing, visual interpretation. Operational workflows can be tailored on the basis of operational scenarios (ports, airfields, urban, lines of communications, industrial compound, etc.).

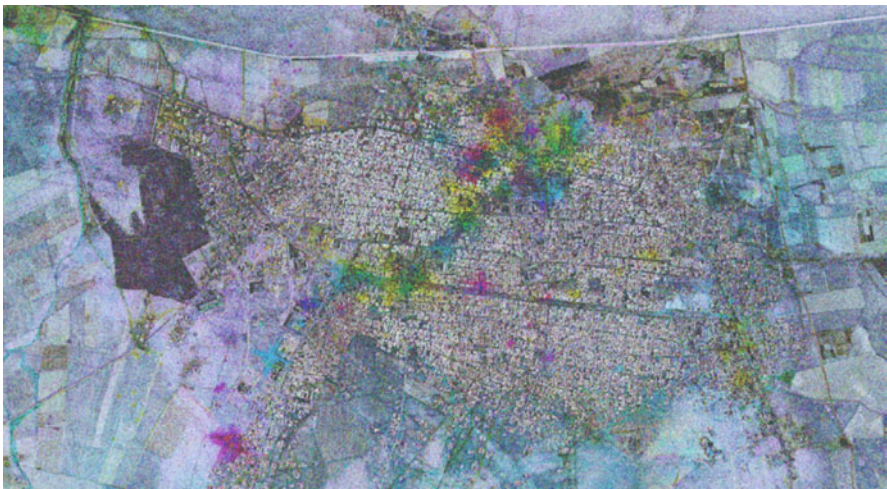
Data preparation are normally executed, thanks to the most common software functionalities already available in the market, e.g., co-registration, phase coherence extraction, geocoding, ortho-rectification.

Data processing would benefit from algorithms and tools available in the market or developed on purpose, according to the need of users, e.g., layover analysis, change detection (amplitude, coherent, or incoherent), edge detection and feature extraction.

The definition of workflows has a twofold advantage. First of all, the workflows become a guided process for imagery analysts through the complex applied physics of the SAR imagery interpretation. Secondly, in the near future, with application of deep learning techniques, it would be possible to train semiautomated systems to execute the workflows, requesting the intervention of the imagery analysts only in case of abnormal behaviors.

Military applications already investigated falls in the domain of damage assessment (Fig. 1), target analysis, monitoring, and military planning.

Significant elements characterizing defense-related SBEO applications have been described, also providing information on more recent developments in this domain.



**Fig. 1** Multicoherence product from the execution of a workflow for damage assessment COSMO-SkyMed image © ASI 2017

The use of adequate satellite constellations with suitable architectural characteristics and possibly in combination with other collection sources is an important enabler. Furthermore, in order to be effective in current operational scenarios, military SBEO applications need to find the proper balance to use modern exploitation and analysis capacities and flexible dissemination chains with the constraints of secure environments typically set up to protect classified information.

---

## **Examples of EO Operational Tasks and Services for Security and Defense**

### **Examples of EO Operational Tasks**

The public domain has the perception of how SBEO works based on what they have seen in the movies rather than in the actual orbital dynamics that govern the movement of the satellites. The inescapable truth is that, once a satellite has been inserted into its orbit, there is not much we can do to control the moment at which it overflies our target of interest other than wait. This introduces a number of caveats that need to be carefully considered when using such systems for security and defense applications. Hence, the expression commonly used by image analysts who say that “when you need an image of a certain location the satellite is usually on the other side of the Earth; and when it finally reaches the desired coordinates, they are always cloud covered.”

Fortunately, while this was usually the case two decades ago, the proliferation of satellite platforms that we have seen in recent years has somehow alleviated this limitation, increasing dramatically the number of passes/day over any given location. However, despite the efforts of some companies that claim to be able to provide imagery every 3 h, we cannot ignore the fact that a satellite does not and will not (for the time being) provide the same live feed as other systems such as RPAS or potentially HAPS, already mentioned above. Thus, although these are increasingly frequent, the views that they provide are still limited to particular instants in time. Thus, the image analysts have developed a series of skills over time that allow make assessments based on hypotheses developed using these views. It would be equivalent to try to understand a movie while only being able to see certain frames.

Image analysts call certain features that they use to elaborate these hypotheses “indicators.” For instance, the sudden appearance of inflatable rubber boats at a makeshift illegal migrant camp located on a specific coastline is an indicator that, even if there are no departures visible on the image yet, there is a very high probability that launches will soon be taking place. Of course, the presence of indicators is very strongly associated to the identification of “patterns of life” or “patterns of behavior.” And these, in turn, are associated with the continuous observation of a location of interest, or what is called “monitoring.” Monitoring allows the analyst to establish a baseline, a visual understanding of the type and level of activity that is common at a certain location. When the analyst sees an event that departs from this usual activity, something that may be called an “anomaly,” an alert

can immediately be triggered and the level of surveillance be increased to identify the causes and possible consequences of such change. Of course, the reliability of the assessment is directly correlated with the duration of the monitoring period, meaning that longer baselines provide better results.

Some examples of this application are the monitoring of military installations, such as ports and airfields, that serve as a baseline for the detection of the deployment of certain types of weapons systems, troops, aircrafts, and vessels that may have strategic implications for the region: arrival/departure of aircrafts and vessels, deployment of SAM or SSM systems, improvement of facilities, development of new infrastructures, identification of the level readiness of the different units occupying the military installations, assessment of their operational status, estimation of their capability, etc.

Another example very commonly related to SBEO monitoring for defense is the field of treaty verification. This was in fact the origin of Open Skies, an initiative signed between the USA and the former USSR at the peak of the Cold War to guarantee support to the mutual assured destruction (MAD) doctrine by providing means to each of the parts to ascertain what the other was doing. Today, satellite imagery is used to monitor the development of nuclear weapons by measuring the level of activity taking place at well-known uranium mines, or monitoring the status of certain processing and enrichment plants or gauging the performance of certain nuclear reactors where plutonium is known to be produced, or assessing the results of nuclear detonations carried out at carefully concealed underground test sites. Monitoring is also the basis for the assessment of a country's strategic outreach in terms of its capacity to project power, either through the deployment of forces or the use of weapons of mass destruction (WMD) and their means of delivery. Other additional requested information, for example, are the capacity and status of their naval units: how many cruiser vessels do they have available; if they are building aircraft carriers: how many, when they will be operational; if they have ballistic missiles: how far they can go, from where are they launched; if it is likely to be another launch test soon: how accurate they are; where are their strategic bombers deployed; and so on.

Monitoring tasks generally account for a significant portion of SBEO applications for security and defense. There are other uses, however, for which intelligence derived from satellite imagery is also critical. One of this use is obviously military planning, an activity which occurs generally before actual events take place. The term coined for this in military parlance is "intelligence preparation of the battlefield (IPB)." There are numerous instances where products derived from images may support the IPB process: terrain reconnaissance, multicriteria cross-country mobility analysis (CCM), identification of Go/No Go areas, visibility analysis, analysis of critical infrastructures, route analysis, contingency planning, training, etc.

Other uses involve the assessment of a situation on the ground after a certain event has taken place, like an airstrike (BDA). Another very frequent post-event application of SBEO is the validation of intelligence obtained through other sources. In this regard, there is an increase of demands that deal with the investigation of illegal activities, including cross-border crime (CBC). A significant amount of these have to do with the trafficking of drugs or weapons, which pose an important security threat to

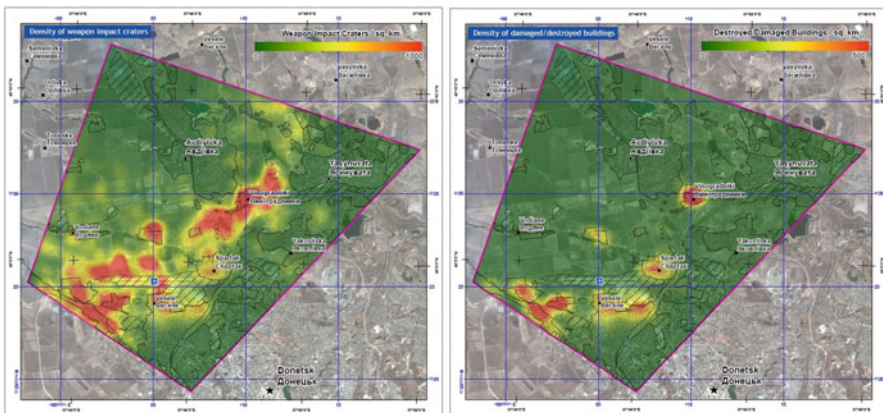
EU Member States. Most of them are related to the existence of vessels, aircraft, trucks, and other means of transportation and the need to confirm their presence at certain locations such as ports, airfields, or border crossing points (Figs. 2, 3, and 4).

The list of examples is obviously nonexhaustive and it leaves out some other plausible uses of SBEO for security and defense. However, we cannot close this section without mentioning one important security application which is the management of the crisis following natural disasters such as earthquakes, wildfires, or floods. In these cases, it is critical to have immediately after the event updated maps and spatial datasets of the theaters of operation which will most likely have changed significantly due to the unfolding of the disaster itself. These datasets will provide the rescue teams with the necessary information to establish priorities and make informed decisions on the ground as soon as possible even before arriving at the disaster area.

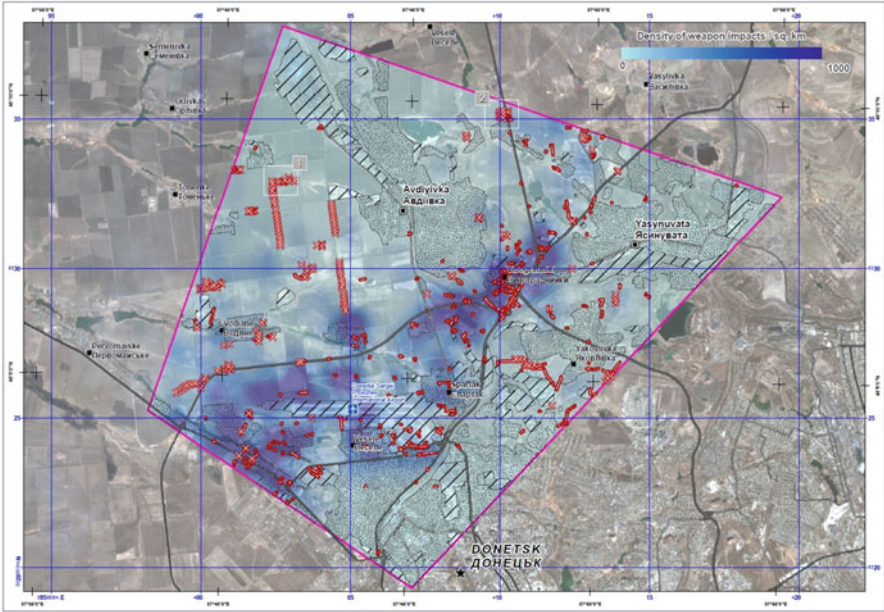
Security and defense operations and information managers will face a wide range of situations involving different requirements and end users. Industry and technological innovation are developing at such a pace that the offer of SBEO services available is increasing exponentially. Now, more than ever, the GEOINT professional needs to amplify his/her domain of knowledge in order to incorporate an understating of the different options available in order to choose that which better satisfies the needs of his/her customers. In most cases, the solution will consist of a mix of different tools, platforms, and sensors that, properly combined, will cover all the aspects of any given situation and provide the most efficient answer.

### Copernicus SEA

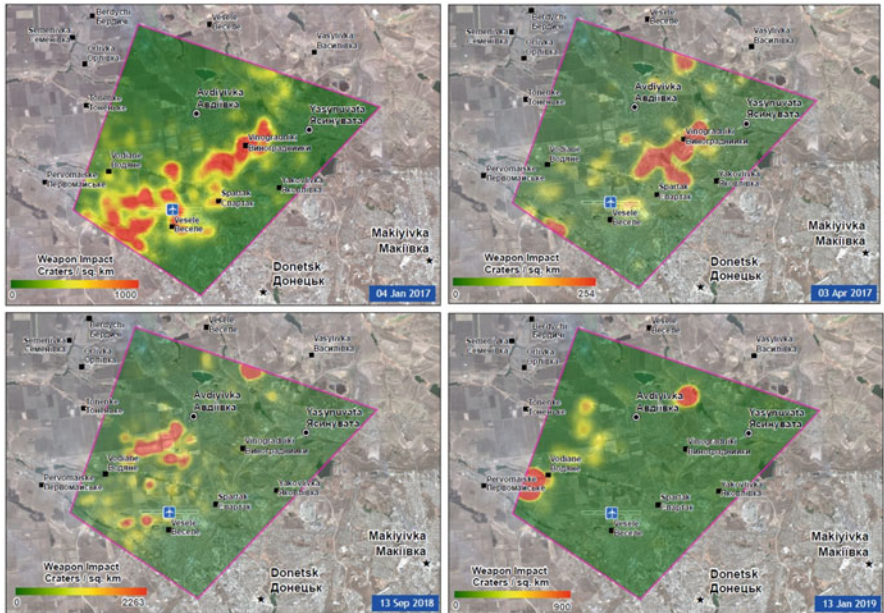
Cooperation between the EU Satellite Centre and the European Commission (EC) is a key enabler for SatCen EO applications development. Such cooperation started more than 10 years ago with a strong involvement of SatCen in the EC research



**Fig. 2** Density maps comparing the weapon impacts visible on the image with the damage to buildings and infrastructures



**Fig. 3** Density map representing weapon impacts overlaid with the different military positions and equipment observed on the image



**Fig. 4** A temporal series representing the evolution of the weapon impacts over the duration of the conflict

projects mainly in the areas of space and security and, in particular, through the FP6, FP7, and finally the H2020 Framework Programme.

The main element of this cooperation has been, and remains, Copernicus and several projects such as LIMES, GMOSAIC, G-NEXT, and BRIDGES that prepared the future operational role of SatCen in Copernicus, setting up the preoperational framework for the services that started in 2017.

Thus, Copernicus Support to EU External Action (SEA) is the result of many years of research and development by SatCen in partnership with the Industry under the European Union’s Framework Programme for Research and Technological Development materialized by the transition of SEA from research and development and preoperational service provision to a fully operational mode.

Copernicus SEA is embedded in the Copernicus programme security component, therefore part of “*the world’s largest single programme for observing and monitoring the Earth, for the ultimate benefit of all European citizens*” (Copernicus Support to Eu External Action Website) (Fig. 5).

Copernicus is composed of three components:

- *The space component.* This includes two types of satellite missions: Copernicus dedicated Sentinels and commercial or other space agencies’ missions, called Contributing Missions (including very high-resolution satellite missions critical for security applications)
- In situ measurements (mainly ground-based providing information on oceans, continental surface, and atmosphere)
- Six services offered to authorized users and public



**Fig. 5** Copernicus Programme structure – Source Commission DG-GROW (Presentation at SEA User Workshop – Paris)



The six services are land, marine, atmosphere, emergency, climate change, and security. Each service is delegated to different “entrusted entities.”

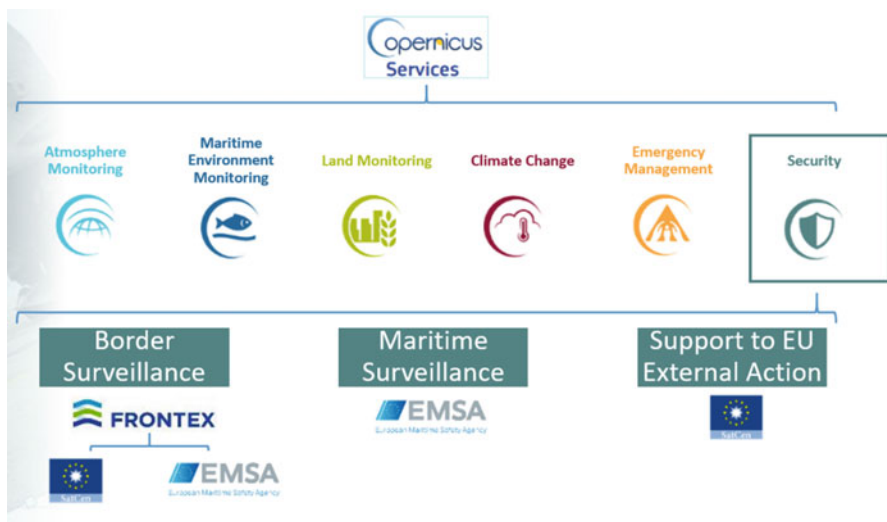
Regarding the Governance, the EC has the overall responsibility of the program, and it is assisted by the Copernicus Committee including Member States, a Security Board (specific configuration of Committee), and a User Forum, as a working group to advise the Copernicus Committee on user requirements aspects (Regulation (EU) No 377/2014 of the European Parliament 2010).

The Security Board is involved in the management of information security for Copernicus and addresses issues such as the cyber security of the space and service infrastructures (Fig. 6).

### Copernicus Security Services

*The security service is to provide information in support of the civil security challenges of Europe improving crisis prevention, preparedness, and response capacities, in particular for border and maritime surveillance, but also support for the Union’s external action, without prejudice to cooperation arrangements which may be concluded between the Commission and various Common Foreign and Security Policy bodies, in particular the European Union Satellite Centre (Regulation (EU) No 377/2014 of the European Parliament 2010).*

In three key areas, i.e., Support to EU External Action, Border Surveillance and Maritime Surveillance, the security service is being implemented by the following entrusted entities: SatCen, FRONTEX, and EMSA. The operations started in 2016 for the Border Surveillance and Maritime Surveillance components of the security service and in May 2017 for the Support to External Action component.



**Fig. 6** Copernicus services (and components in security). (Source Commission DG-GROW)

SatCen's main contribution is materialized by the role of entrusted entity for the operations of the Copernicus service in Support to EU External Action (SEA); SatCen also supports Border Surveillance through a Service Level Agreement with FRONTEX.

SatCen is thereby entrusted with the operational management of the Copernicus SEA service. Today, SEA addresses service production mainly through issuing and management of industrial service contracts such as a Framework Contract for "Geospatial production" but also the production of sensitive layers of information by image analysts and quality checks at SatCen. In addition, SEA implements user uptake activities mainly for the enlargement of the user base as well as service evolution activities taking benefit of state of the art in research and technological developments. For user uptake activities at least two workshops are organized per year. SatCen also implements a focal point for service's "Authorised Users" in the "SatCen Brussels Office." Security consideration regarding the requests is fully taken into account as each request is evaluated by the SatCen Tasking Authority (EEAS) from the sensitivity point of view. As Copernicus SEA does not currently manage EU Classified Information (EUCI) (2013/488/EU 2013), if a request is considered too sensitive and needs to be classified, it could be managed, if relevant, outside the perimeter of Copernicus as a SatCen classified task.

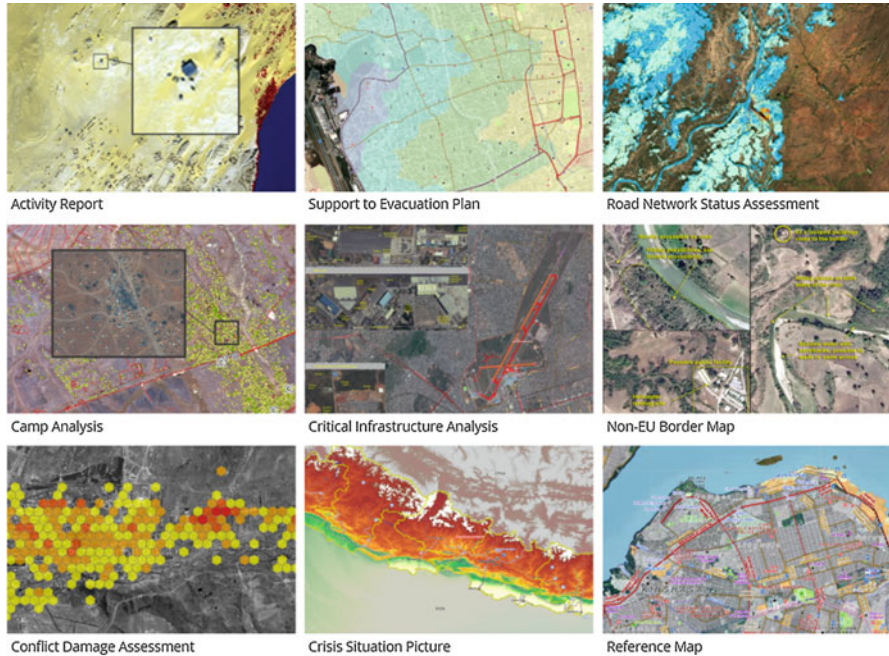
SEA's objective is to assist the EU and its Member States in civilian missions, military operations, and interests outside EU territory. It is designed to support the EU by improving the situational awareness of European Commission, European External Action Service, and Common Security and Defence Policy stakeholders including the Member States. The service can be activated to respond within very short timescales, as is necessary in cases of responses to crises such as political or armed conflicts. On the other hand, it is possible for the service to carry out monitoring campaigns over longer periods of time in order to develop a picture of how phenomena on the ground are changing. The primary target users are European entities, the EU, and Member State Ministries of Defence and Foreign Affairs as well as key international stakeholders, as appropriate under EU international cooperation agreements such as United Nations.

### **SEA Service Portfolio**

After a ramping up of the service, SEA reached its full operational state in 2018 with, as mid-2019, more than 140 activations received from authorized users from EU Institutions, in particular EEAS and Member States. SEA products were built using mainly Copernicus Contributing missions as well as Sentinels satellites data as complementary sources (Fig. 7).

Mid-2019, the SEA service is mainly activated by the EU External Action Service: from the nine services of the portfolio, seven have been used so far (Fig. 8).

Analysis of EO data based on different techniques is used to identify patterns of illegal activity in an area of interest. Optical very high resolution (VHR) imageries are used to identify vehicles and infrastructure potentially suspicious. Radar Sentinel imagery interferometry techniques are used to identify the use of paths and roads during a time lapse.



**Fig. 7** SEA service portfolio. (Source SatCen (European Defence Action Plan – COM 2016))

## Evolution of EO Services and Application at EU SatCen and Copernicus SEA

### SatCen Service Evolution: Artificial Intelligence/Machine Learning

The concept of artificial neural networks and the theory of how these could be applied to a number of different applications, particularly in the field of EO and remote sensing, have been deeply described in the previous paragraphs. The development of the computing power necessary to drive this major breakthrough has reached critical mass, thanks to the continuous increase of chip capacity. Moreover, big data must be carefully stored over years of increasing generation and ingestion of information. But big data in itself is not useful. It only acquires a meaning if we are able to exploit it in such a way that it allows us to identify patterns, understand behaviors, bring to the surface the hidden structure of a certain phenomenon, and even predict what is going to happen next. It is particularly important in the field of Artificial Intelligence and Machine Learning (AI/ML) because for the first time SBEO service providers such as EU SatCen have accumulated enough data to train the algorithms to such an extent that they will provide meaningful, reliable, and actionable results. And once they are trained, the expectations are that these



**Fig. 8** Example of an SEA activity analysis product for detecting smuggling and other illegal activity. (Source SatCen – SEA product portfolio (Copernicus website [www.copernicus.eu](http://www.copernicus.eu)))

algorithms will be able to breeze through the data and draw conclusions that would otherwise take an unfeasible amount of time for a human to reach.

There are numerous situations in the field of SBEO where AI/ML is already being used. Experience has shown that the algorithms are particularly efficient at performing repetitive tasks that may seem pretty straightforward in terms of complexity but often excruciatingly tedious for an analyst, such as scanning an image in search of changes or looking for certain objects like armored vehicles, aircraft, air defense sites, or other sorts of military equipment. At the EU SatCen, for example, it is not considered a future scenario in which the machine will eventually end up substituting the human analyst. There is a strong belief that certain traits which are common in successful image analysts, such as the capacity to unveil causal associations between elements on the image, or the ability to understand spatial relationships, or the facility to elaborate probable hypotheses to explain what is being observed, will very hardly, if ever, be outperformed by a machine. Thus, what is envisaged as a more likely scenario is one where the image analyst takes full advantage of the power of AI/ML to automate tasks such as automatic change detection and automatic feature detection and only intervene when the algorithms flag an alert, to alert that some relevant event has been found. This idea, which is sometimes known as a “tip and cue” approach, may fit surprisingly well with a

hybrid SBEO collection plan which could include a mix of different sensors with complementary capabilities. As an example, to illustrate this, consider a situation where access is guaranteed to a constellation of microsatellites that provides fresh imagery at a medium spatial resolution but very high cadence, e.g., 3 m pixels every 2–3 h. The precision given by a 3 m pixel may not be enough to identify the type of equipment present on the ground, but if you know already what you are dealing with because of higher resolution imagery acquired at an earlier date, the medium resolution-high cadence imagery may be more than enough to highlight a change in the level of activity and trigger an alert. The analyst can then use the awareness of this event to tip off another constellation with higher precision sensors and program an acquisition with a better spatial resolution, and then may confirm the assessment. If the identification of the changes that triggers this mechanism can be done automatically by an AI/ML neural network, the analyst can significantly increase the area of surveillance and wait for these alerts to pop up, thus covering a larger surface and using his skills more wisely.

## Copernicus SEA Service Evolution

Within the Copernicus Security Service component, the service evolution aims at promoting changes to the Service, aligned with the overall Copernicus strategy. The goal is to improve the existing portfolio of services by adding or modifying existing products or by implementing changes within the production or activation and delivery systems that improve the overall service experience to the users.

First, Copernicus SEA service is constantly adapting its response to the upcoming applicable policies, in particular those policies governing the EU External Action such as the EU Global Strategy for the European Union's Foreign and Security Policy and the Space Strategy for Europe, both issued in 2016. Any other relevant EU Policy will be considered as well.

Space Strategy for Europe (Space Strategy for Europe – European Commission COM 2016) states that *“Additional services will be considered to meet emerging needs in specific priority areas, including . . . (ii) Security and Defence to improve the EU's capacity to respond to evolving challenges related to border control and maritime surveillance with Copernicus and Galileo/EGNOS. This expansion will take account of new technological developments in the sector, the need to ensure adequate level of Security of the infrastructure and services, the availability of different data sources, and the long-term capacity of the private sector to deliver appropriate solutions.”*

European Defence Action Plan (European Defence Action Plan – COM 2016): *“The Commission shall explore how Copernicus could cover further Security needs, including Defence. It shall strengthen Security requirements and will reinforce synergies with non-space observation capabilities in 2018.”*

In the Space Strategy for Europe, additional services are considered in the area of security and defense. To some extent, the Copernicus SEA service could be considered as already implementing new services for defense and security, and therefore in

line with the EDAP orientations (Member States defense users and CSDP military operations being part of the SEA users whenever they request to access the service within the context of the Common Foreign and Security Policy). The EDAP provides guidance on possible future evolution, in particular regarding the strengthening of security requirements and re-enforcing synergies with nonspace observation capabilities; this guidance shall be taken into account for the evolution of the Copernicus SEA service.

Nevertheless, SEA shall also be made available to new users having a bearing on the EU External Action. Copernicus SEA workshops, in particular the workshop organized in Paris at CNES (Centre National d'Études Spatiales) in December 2018, clearly highlighted that there are many potential new users in areas such as Ministry of Interior, Ministry of Foreign Affairs, maritime security actors, and agencies such as EFCA and EUROPOL that could get benefit from the service. Those users would need an easy access to the service, and this will have to be taken into account for its evolution. Regarding maritime security, it is worth mentioning the "European Union Maritime Security Strategy" (On 24 June 2014 the General Affairs Council of the European Union approved the "European Union Maritime Security Strategy" (EUMSS) 2018) endorsed by the EU Council. Its action plan revised in June 2018 specifically target *Support the conduct of CSDP missions and operations in the global maritime domain with EU maritime surveillance assets.* ("In line with CISE (Common Information Sharing Environment (A common information-sharing environment (CISE))), ensure consistency and strengthen coordination between the existing and planned maritime surveillance initiatives on the basis of existing programs and initiatives by EDA, EFCA, EMSA, EUSC, FRONTEX, and other European agencies (e.g. ESA) as well as the Earth Observation programme (Copernicus), GALILEO/EGNOS (European Geostationary Navigation Overlay Service), and other relevant projects and initiatives. [MS/COM/EEAS/EDA]").

Second, Copernicus SEA is strongly user driven and their requirements are fully taken into account both regarding the access to the service as well as the extension of the service portfolio.

Considering the rationale behind the Copernicus SEA, a set of predefined products has been defined and compiled in the Copernicus SEA portfolio, offering EU and international actors an initial pool of services that aim to tackle their needs in crisis situations or emerging crisis.

Service evolution is to bring new products to the users by extending SEA portfolio of services. Emerging requirements have been expressed, for example, in the areas of cultural heritage, illegal crop monitoring, security of EU/international events.

New products are achieved by finding new methods to exploit existing sensors by retrieving new types of information as well as exploiting new sensors and data. SEA service evolution demonstrated, for example, that the use of Copernicus Sentinels satellites was useful as complementary data based, for example, on the following capabilities: the revisit time of Sentinel-2, interferometry with Sentinel 1 to detect small changes in specific areas such as deserts, sea, etc.

Interagency cooperation is also a driver of innovation in this context, and it is worth mentioning the SatCen/EDA GeoHub project that is building a geo-spatial portal as well as the REACT project (briefly described previously ([IAC-14-B1.5.4 Cosmo-Skymed data utilization and applications](#))) on the exploitation of SAR data. Both projects could be beneficial for SEA service evolution, as synergies are already well established.

Regarding the access to the service, SEA is currently benefiting from the infrastructure already in place at EU SatCen. The new developments planned for the infrastructure are aimed to provide the necessary hardware/software infrastructure to enable and optimize the management of the Copernicus SEA service, including activation workflow; seamless production and publishing; easier request and access to the products by the users. In the future, this infrastructure will need to be adapted to a considerable increase in data sources and volume, both for Earth observation and additional data, such as in situ, open source, etc. Additionally, the mentioned infrastructure must adapt to the need to “strengthen security requirements” and to “cover further security needs, including defense” (c.f. EDAP (European Defence Action Plan – COM 2016)) which might have an impact on the infrastructure in terms of the reinforcement of the capacity to process sensitive data.

Service evolution of this first phase of Copernicus SEA for the period 2014–2020 is currently extending the user community, the service portfolio, and is facilitating the access to the service.

SatCen is currently preparing with its partners the next phase of SEA within addressing “Copernicus 2.0” for the period 2021–2027, taking benefit of the results and lessons learned of service evolution during the first phase. A particular attention will be given to common requirements, interagency cooperation, interactive access through geo-portal, innovative tools such as artificial intelligence, and the availability of new space and nonspace sensors.

---

## Conclusion

This chapter identified the current and future trend in the domain of Space-based Earth Observation (SBEO) from a security and defense perspective. Starting from a high-level state of the art, the current security and defense general needs have been described, pointing out how the future SBEO capabilities will be changed by the current new military scenario as well as the new space economy. In particular, the center of gravity will be more and more moved to the ground segment, always keeping in mind the specific military requirement of confidentiality, integrity, and availability of IMINT information.

Any SBEO capability shall be adapted for ad hoc security and defense environments, without necessarily implying different design but with enforcement of specific security standard protocols and restrictions, aiming to the interoperability and integration of different sources. The use of commercial and unsecured outflows can in any case represent a valid contribution that indeed needs to be properly balanced.

Considering the duality and increasing synergies between homeland security and external actions, the challenge will be in the implementation of a coordinated and holistic approach avoiding unnecessary duplication.

Some example of SBEO tasks and applications have been described, showing how the management of Artificial Intelligence and Machine Learning services will need to be properly customized to improve the inalienable analysts' skills, expensive, and precious resources that can be increased exponentially with tailored tools and related services.

Security domain, based on the experience of Copernicus Programme and EU SatCen services, nowadays is working with a cooperative model, delivering effective results in many applications.

This cooperative model has not yet reached the same level of maturity in the defense domain. However, significant efforts are conducted by national MoDs to cooperate on specific needs and activities. A further step forward might be a "pooling and sharing" model's application.

Furthermore, more support and contribution from EU institutions, eventually taking advantage of the security domain experience, tools, and facilities, might provide added value and cost benefit in the challenge of implementing a more structured and coordinated approach even in the defense domain.

The development of new common SBEO platforms/services could represent a first example (or the second one if we consider Galileo Public Regulated Service) of a European system to support defense needs of EU Member States.

---

## References

- 2013/488/EU: Council Decision of 23 September 2013 on the Security rules for protecting EU classified information – Article 2: 'EU classified information' (EUCI) means any information or material designated by a EU Security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States'
- A common information-sharing environment (CISE) is currently being developed jointly by the European Commission and EU/EEA members with the support of relevant agencies such as the EFCA. It will integrate existing surveillance systems and networks and give all those authorities concerned access to the information they need for their missions at sea. (Source: <https://www.efca.europa.eu/en/content/common-information-sharing-environment-cise>)
- Adams J, Gillespie A (2006) Extracting information from spectral images. In: Remote sensing of landscapes with spectral images: a physical modeling approach. Cambridge University Press, Cambridge, pp 1–38
- Arel I, Rose DC, Kamowski TP (2010) Deep machine learning – a new frontier in artificial intelligence research. *Comput Intell Mag IEEE* 5:13–18
- Atkinson PM, Tatnall ARL (1997) Introduction neural networks in remote sensing. *Int J Remote Sens* 18(4):699–709
- Ball JE, Anderson DT, Chan CS (2017) Comprehensive survey of deep learning in remote sensing: theories, tools, and challenges for the community. *J Appl Remote Sens* 11(4):042609-1–042609-54



- Belward AS, Skøien JO (2015) Who launched what, when and why; trends in global land-cover observation capacity from civilian earth observation satellites. *ISPRS J Photogramm Remote Sens* 103:115–128
- Bovolo F, Bruzzone L (2015) The time variable in data fusion: a change detection perspective. *IEEE Geosci Remote Sens Mag* 3(3):8–26
- Britz M, Eriksson A (2005) The European security and defence policy: a fourth system of European foreign policy? *Polit europeenne* 3(17):35
- Câmara G, Ferreira Gomes de Assis LF, Queiroz G, Reis Ferreira K, Llapa E, Vinhas L, Maus V, Sanchez A, Cartaxo Modesto de Souza R (2016) Big Earth Observation data analytics: matching requirements to system architectures. *BigSpatial16*, Oct 31–Nov 03 2016, Burlingame. <https://doi.org/10.1145/3006386.3006393>
- Campbell JB, Wynne RH (2011) *Introduction to remote sensing*. Guilford Press; 5th edition (June 21, 2011). ISBN-10: 160918176X ISBN-13: 978-1609181765. p 667
- Committee on Earth Observation Satellites [www.ceos.org](http://www.ceos.org)
- Copernicus Support to Eu External Action Website. <https://sea.security.copernicus.eu/>
- Copernicus website. [www.copernicus.eu](http://www.copernicus.eu)
- Denis G, de Boissezon H, Hosford S, Pasco X, Montfort B, Ranera F (2016) The evolution of Earth Observation satellites in Europe and its impact on the performance of emergency response services. *Acta Astronaut* 127:619–633
- Denis G, Claverie A, Pasco X, Darnis J-P, de Maupeou B, Lafaye M, Morel E (2017) Towards disruptions in Earth observation? New Earth Observation systems and markets evolution: possible scenarios and impacts. *Acta Astronaut* 137:415–433
- EU Capability Development Plan 2018
- European Defence Action Plan – COM (2016) 950 final – Nov 2016
- European External Action Service – A Global Strategy for the European Union’s Foreign and Security Policy, Jun 2016
- Fitness tracking app Strava gives away location of secret US army bases. <https://www.theguardian.com/world/2018/jan/28/fitness-tracking-app-gives-away-location-of-secret-us-army-bases>. Last access Apr 2019
- French white paper on Defence and National Security – 2013
- Fukuyama F (1989) The end of history? *Natl Interest* (16):3–18, Summer
- Fulcher BD, Little MA, Jones NS (2013) Highly comparative time-series analysis: the empirical structure of time series and their methods. *J R Soc Interface* 10:20130048
- Ghassemian H (2016) A review of remote sensing image fusion methods. *Inf Fusion* 32:75–89
- Hepner GF, Logan T, Pitter N, Bryant N (1990) Artificial neural network classification using a minimal training set: comparison to conventional supervised classification. *Photogramm Eng Remote Sens* 56(4):469–473
- Holmes C, Tucker C, Tuttle B (2018) GEOINT at platform scale. In: *The state and future of GEOINT 2018*. Published by The United States Geospatial Intelligence Foundation USGIF, Herndon, pp 1–38
- [https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-04-03-factsheet\\_react](https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-04-03-factsheet_react). Last visit Mar 2019
- [https://www.eda.europa.eu/what-we-do/activities/activities-search/persistent-surveillance-long-term-analysis-\(sultan\)](https://www.eda.europa.eu/what-we-do/activities/activities-search/persistent-surveillance-long-term-analysis-(sultan)) Last visit Mar 2019
- Hussain M, Chen D, Cheng A, Wei H, Stanley D (2013) Change detection from remotely sensed images: from pixel-based to object-based approaches. *ISPRS J Photogramm Remote Sens* 80:91–106
- IAC-14-B1.5.4 Cosmo-Skymed data utilization and applications
- Lee J-G, Kang M (2015) Geospatial Big Data: challenges and opportunities. *Big Data Res* 2(2):74–81
- Li J, He Z, Plaza J, Li S, Chen J, Wu H, Wang Y, Liu Y (2017) Social media: new perspectives to improve remote sensing for emergency response. *Proc IEEE* 105(10):1900–1912

- Lillesand T, Kiefer RW, Chipman J (2014) Remote sensing and image interpretation. Wiley, Hoboken, p 704
- Long Y, Gong Y, Xiao Z, Liu Q (2017) Accurate object localization in remote sensing images based on convolutional neural networks. *IEEE Trans Geosci Remote Sens* 55(5):2486–2498
- Maggiori E, Tarabalka Y, Charpiat G, Alliez P (2017) Convolutional Neural Networks for Large-Scale Remote-Sensing Image Classification *IEEE Transactions on Geoscience and Remote Sensing* 55(2):645–657
- MCRP 2-10B.5 Imagery Intelligence – US Marine Corps
- Nativi S, Mazzetti P, Santoro M, Papeschi F, Ochiai O (2015) Big Data challenges in building the Global Earth Observation System of systems. *Environ Model Softw* 68:1–26
- On 24 June 2014 the General Affairs Council of the European Union approved the “European Union Maritime Security Strategy” (EUMSS), Following the mandate by EU heads of state or government. The EUMSS action plan was recently revised (26 June 2018). This document provides guidelines regarding COM, EEAS and agencies (including SatCen) cooperation in the EUMSS framework. [https://ec.europa.eu/maritimeaffairs/policy/maritime-security\\_en](https://ec.europa.eu/maritimeaffairs/policy/maritime-security_en)
- Popescu et al. Cloud computing case studies and applications for the space and security domain. European Union Satellite Centre
- Regulation (EU) No 377/2014 of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010
- Space Strategy for Europe – European Commission COM (2016) 705 final – October 2016
- Toth C, Józków G (2016) Remote sensing platforms and sensors: a survey. *ISPRS J Photogramm Remote Sens* 115:22–36
- Tzu S (2007) *The art of war*. Filiquarian, First Thus edition. ISBN-10: 1599869772
- United Nations Treaties and Principles on Outer Space (2002) United Nations, New York. United Nations publication, Sales no. E.02.I.20. ISBN 92-1-100900-6
- US Joint Publication – Joint Intelligence – 22 October 2013



# Satellite EO for Disasters, Risk, and Security: 39 An Evolving Landscape

Helene de Boissezon and Andrew Eddy

## Contents

Introduction .....	734
Satellite-Based Earth Observation: An Increasingly Critical Asset for Risk Management and Security .....	735
The Copernicus Emergency Management Service: The Hurricane Irma Example .....	735
Risk and Risk Mitigation .....	746
Evolving Supply and Hot Topics for Security .....	750
Conclusions .....	756
References .....	757

## Abstract

The number of EO satellites is growing rapidly, doubling in the last 10 years. Their data are increasingly integrated into comprehensive services such as the Copernicus Emergency Management Service, which offers full-cycle support for disasters in Europe and internationally. Nevertheless, widespread operational application of satellite EO to disasters concerns response and rapid mapping, focused on hazard information rather than risk reduction. New satellite missions offer increased capabilities, and organizations such as CEOS are initiating pilots with users for risk reduction and resilience building. Financing the value-added component remains a challenge.

---

H. de Boissezon (✉)  
French Space Agency (CNES), Toulouse, France

Committee on Earth Observation Satellites (CEOS), Haiti Recovery Observatory,  
Port au Prince, Haiti  
e-mail: [helene.deboissezon@cnes.fr](mailto:helene.deboissezon@cnes.fr)

A. Eddy  
Athena Global, Simiane-la-Rotonde, France  
e-mail: [andrew.eddy@athenaglobal.com](mailto:andrew.eddy@athenaglobal.com)

## Introduction

Over the past decade, the world of satellite-based Earth Observation (EO) has changed dramatically. From roughly 150 EO satellites in 2008, to over 350 in 2018, the number of observing sensors has more than doubled. This number excludes microsats and CubeSats, representing a further 330 (Pixalytics, 2018). Furthermore, that number is expected to double again in the next decade. Larger satellites continue to be replaced by more flexible constellations of smaller satellites, offering greater reach and scope, and greatly improved revisit time. Planet Labs alone now images the entire Earth every day. Even more striking is the range of observations that are being acquired. Whereas a decade ago, few satellites offered very advanced capabilities with sensors other than high-resolution optical or medium-resolution multispectral sensing, today, there are scores of satellites offering complex data requiring advanced processing and interpretation skills. Progress is also being made in making these tools and skills available to more people – through open data and licensing policies – and in bringing training on these easier-to-access tools to more people. In summary, the offering put forward by satellites has never been richer and more diverse, or more readily available.

Ironically, this enlarged offering brings an added complexity: choice. Not all sensors are equal; many applications require multiple sensors and different data sets. A whole research field has emerged in how to properly and most expertly fuse data for various applications. Furthermore, even finding the right data set with so much on offer is a challenge.

Gradually, users of satellite EO have enhanced their understanding of how satellites can be used, and new communities of users are emerging. When the French Space Agency CNES and the European Space Agency (ESA) created the International Charter Space and Major Disasters in 1999, providing near-real-time data during and immediately after major catastrophes was an innovation. Today, after some 20 years, 17 agencies regularly contribute to some 40–50 activations in any given year. Sister services have spawned in Asia (Sentinel-Asia) and Europe (Copernicus Emergency), providing strong regional hubs to address more events of regional and national impact.

The Global Facility for Disaster Reduction and Recovery (GFDRR), created in 2006, now boasts 37 member countries and 11 international organizations. Working in close coordination with the World Bank, GFDRR has greatly increased our understanding of how technologies and satellites in particular can be applied to risk reduction, in order to prevent natural hazards from becoming human catastrophes. Still more recently, Copernicus created the Risk and Recovery Program within its Emergency Management Services (EMS), which in addition recognizes that the specific needs of recovery can now also be met at an operational level by satellites. This requires effort to be applied to understanding user needs and offering pertinent EO-based services to those needs, and applying resources from the satellite community address them.

UNOSAT, UNITAR's operational satellite program, created in 2001, provides crisis and impact assessment and situational awareness during disasters but also

offers expanded satellite-related capacity building and training throughout the developing world. UNOSAT aims to make satellite solutions and geographic information easily accessible to the UN family and to experts worldwide and more recently has provided operational support during Post-Disaster Needs Assessments (PDNAs), in conjunction with the EU's Joint Research Centre (JRC) and the World Bank, contributing to Disaster Recovery Frameworks.

Beginning in 2014, the Committee on Earth Observation Satellites (CEOS), an organization representing all the world's major space and remote-sensing agencies, created a permanent Working Group on Disasters with a view specifically to generating a comprehensive strategy for applying EO to Disaster Risk Management. The WG quickly established a series of thematic pilots aimed at exploring how satellite data could be applied to risk reduction more effectively, addressing one of the key priorities of the Sendai Framework. As the principal body bringing together the world's leading satellite agencies interested in EO, CEOS has a key role to play in encouraging the use of satellite EO for risk management and security.

The plethora of new resources applied to the satellite sector has concentrated on data provision according to increasingly demanding specifications, but very little dedicated funding has been applied downstream to making these data part of integral solutions for dedicated disaster and security systems. Until now, the burden of understanding what is available and integrating it into new and existing systems has been borne by the end user, with varying degrees of success. Recently, as the major satellite operators and distributors consider the next generation of services, leaders such as the European Commission have recognized the need for turnkey applications of satellite data tied to disasters and security. Trailblazing services such as the Copernicus EMS open new opportunities to grow awareness of satellite data use within user communities and, in turn, foster new service growth based on existing satellites.

This paper will review how satellite EO is applied to natural hazards in particular in the Copernicus EMS program, arguably the most mature service applying these technologies, and how these services are called to evolve to address the broader risk equation of hazards, exposure, and vulnerability. It will also review some emerging topics of interest to the disasters and security community, including new missions, and fora where leading organizations meet, as well as recent service innovations.

---

## **Satellite-Based Earth Observation: An Increasingly Critical Asset for Risk Management and Security**

### **The Copernicus Emergency Management Service: The Hurricane Irma Example**

As stated on the Copernicus website, Copernicus EMS provides information for emergency response in relation to different types of disasters, including meteorological hazards, geophysical hazards, deliberate and accidental man-made disasters, and other humanitarian disasters as well as prevention, preparedness, response, and recovery activities. While the service is focused on response, it is in fact a full-cycle

service, offering components to address each phase of the disaster cycle. The emphasis is placed on information, rather than data. The service integrates data from a range of sources and provides information products relevant to end-user communities. The innovation in Copernicus EMS is that it is composed of an on-demand mapping component applied to all the aforementioned phases, as well as an early warning and monitoring components. This latter includes systems for floods, droughts, and forest fires. These early warning services are treated in section “[Copernicus EMS Early Warning: EFAS-GLOFAS and EFFIS-GWIS](#).”

In considering how satellite EO is applied to disasters and security, at first the rapid mapping component will be considered in detail and then the risk and recovery mapping component through the experience of the Irma Hurricane in France.

### **Copernicus EMS Rapid Mapping Service**

The Copernicus EMS provides a complete portfolio of mapping products, including maps for reference, delineation, grading, and early monitoring. The response service is a 24/7 service operational 265 days a year, offering products to end users within a few hours of satellite overpass. It was this service that was activated in response to Hurricane Irma.

Hurricane Irma struck the French Caribbean Islands of St. Martin and St. Barthelemy on September 5 and 6, 2017. On St. Martin, the storm caused a crisis involving all areas of governance, including law and order, networks and essential infrastructure, information, and communications. St. Martin was hit by torrential rains and sustained winds of up to 297 km/h. Within the French Civil Security ministry (Ministry of the Interior), the Inter-ministerial Operational Center for Crisis Management or COGIC put itself on alert in “anticipation (of a) potentially catastrophic event” on September 4, as a result of the 5-day National Hurricane Center and Météo France forecasts. After Irma’s landfall, the COGIC raised its alert level 1 to level 2 and then 3 (maximum mobilization), in order to manage an unprecedented situation in the French Caribbean (Fig. 1).

The Irma crisis affected all sectors of public activity. The electricity network was severely damaged: the exposed parts were destroyed and buried parts near the sea significantly damaged; the water network was out of order; the telecommunications network no longer functioned, whether via antennas or submarine cables. Roads were littered with trash, metal sheets, fallen trees, and other debris. To add anxiety to the desperation of the inhabitants, much looting and physical abuse followed this drama, which left a total of 11 victims. This lasted 4 days until the massive arrival of police. The relief operations were colossal, with nearly 2500 police personnel deployed to the scene. The COGIC, meanwhile, remained mobilized at full capacity on 24-h duty, nonstop during the September 6–20 period.

Support mechanisms for the crisis response by satellite imagery worked perfectly: Copernicus Emergency Rapid Mapping Service and the International Charter Space and Major Disasters were activated early on the morning of September 5 (1 day before the hurricane) by COGIC, French Authorized User, on St. Martin and St. Barthelemy. Thanks to their coordinated action, satellite imagery was acquired from the very first hours of the crisis, and cartographic products to support relief efforts

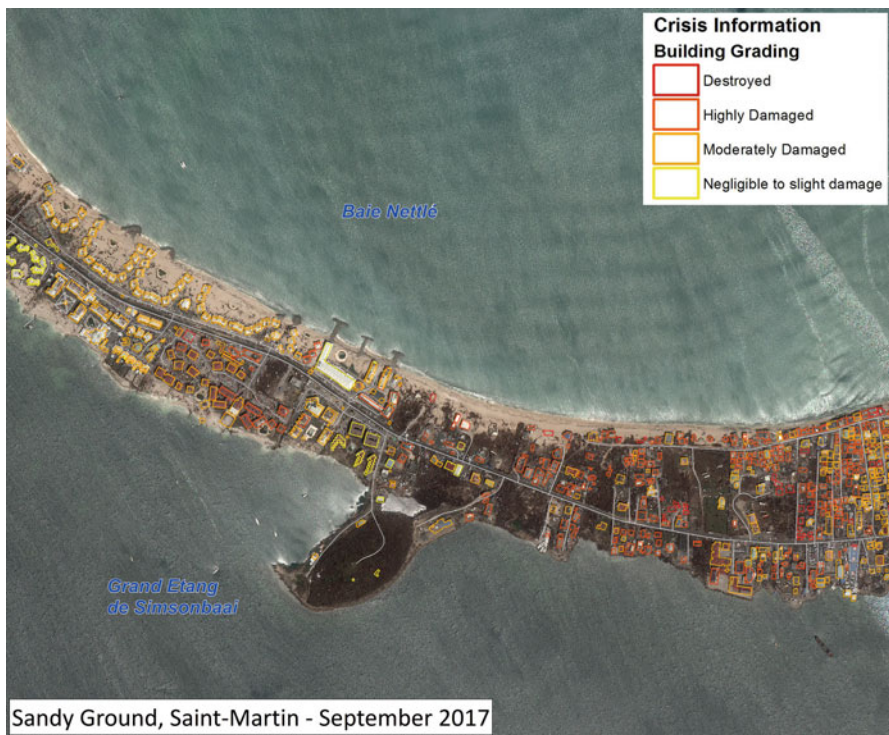


Fig. 1 Copernicus satellite-based damage grading product, St. Martin, September 2017. (Courtesy of Copernicus)

were delivered within 12 h of imagery reception for Copernicus products and 6 h for Charter products.

The French Space Agency (CNES) also decided to program Pleiades very high-resolution (70 cm) acquisitions beyond the standard Charter/Copernicus requests, guaranteeing daily acquisitions from September 7 to 16. The images were available 3 h after acquisition and immediately transmitted to the COGIC and the rapid mapping operator. Within hours, these images were analyzed to provide zoning for damage and impacts and to help organize relief (Fig. 2).

The Irma impact assessment information within COGIC was more than 95% based on satellite imagery and derived mapping. COGIC also produced an atlas at 1/5000 scale presenting “before/after” scenes based on Pleiades images and an exposure database with information on buildings, networks, etc. These same Pleiades images were also used by the Caisse Centrale de Réassurance (national public reinsurer) to provide a first quantification of the direct economic damage. Through the expertise of ICube-SERTIT, a French specialist in satellite-based analysis for crisis management support, the Caisse cross-referenced damaged buildings and insured exposure. The Copernicus and Charter products were also used by the



**Fig. 2** Copernicus satellite-based damage grading product, St. Martin, September 2017, Sandy Ground Close-up. (Courtesy of Copernicus)



European Commission in the evaluation of the French request addressed to the Solidarity Fund of the European Union.

Copernicus EMS Rapid Mapping is a standard service provided by the European Commission. It has been activated more than 350 times since 2012.

### **Copernicus EMS Risk and Recovery Mapping Service**

The Risk and Recovery Mapping Service addresses aspects outside the immediate response phase. It aims to provide generic risk-related information and specific products tied to recovery from disasters. It consists of the on demand provision of geospatial information. This information addresses prevention, preparedness, disaster risk reduction, or recovery phases (product delivery in weeks/months). The user may request products choosing from a pre-defined set of detailed topographic features and disaster risk information (hazard, exposure, risk) and/or describing in free text the information needs specific to the given situation and type of product wanted.

In the case of Hurricane Irma, beyond the crisis phase, satellite-based EO data has largely contributed to piloting and monitoring reconstruction post-Irma, through the comprehensive monitoring of the affected areas over many months. The main issues related to monitoring recovery are complex in a very densely populated territory, taking into account the risks, adaptation of infrastructures, and support to rapid economic recovery. The intensity of this Copernicus EMS Risk and Recovery postcrisis monitoring was unprecedented. On October 2, 2017, CNES decided to secure Pleiades acquisitions over St. Martin and St. Barthelemy for the following months and offered its support to the Inter-ministerial Delegation for Reconstruction and to the DEAL Guadeloupe (Regional directorate for equipment, planning and housing) for EO data to contribute to reconstruction efforts. The delegation, created by decree on September 12, 2017, had the mission to design and coordinate the actions related to the reconstruction of the two islands and their resilience to natural risks and climate change. The delegation and DEAL expressed an interest in continued access to Pleiades until 2020 on St. Martin, in order to precisely measure the necessary reconstruction effort, in support of the technical teams in charge of risk. All Pleiades images, orthorectified according to the national cartographic reference system, have been made available via the GeoPortail IGN (French National Geographic Institute) for the decentralized services of the state in Guadeloupe.

In February 2018, the Inter-ministerial Delegation for Reconstruction activated the Copernicus EMS Risk and Recovery Mapping (RRM) service over the two islands in order to obtain regular mapping, from March 2018 to September 2019, of building and storage area status, as well as rubble, shipwrecks, and improvised dumps. The products use images from Copernicus Third Party Missions, commercial data from partner states made available free of charge for Copernicus contractors, as well as for authorized users. In parallel, CNES decided to continue Pleiades programming on both islands (Figs. 3 and 4).

Copernicus RRM products were first produced at the end of March 2018. In order to contribute to the preparatory work for the fifth Inter-Ministerial Committee

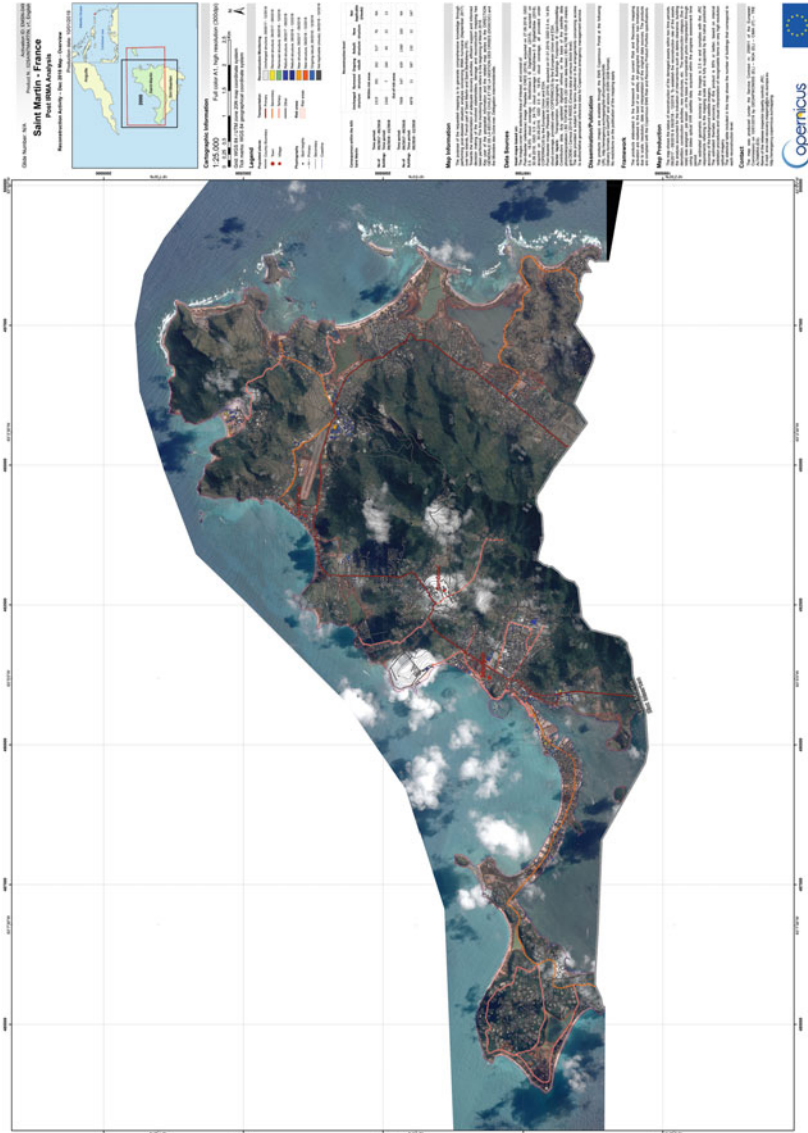
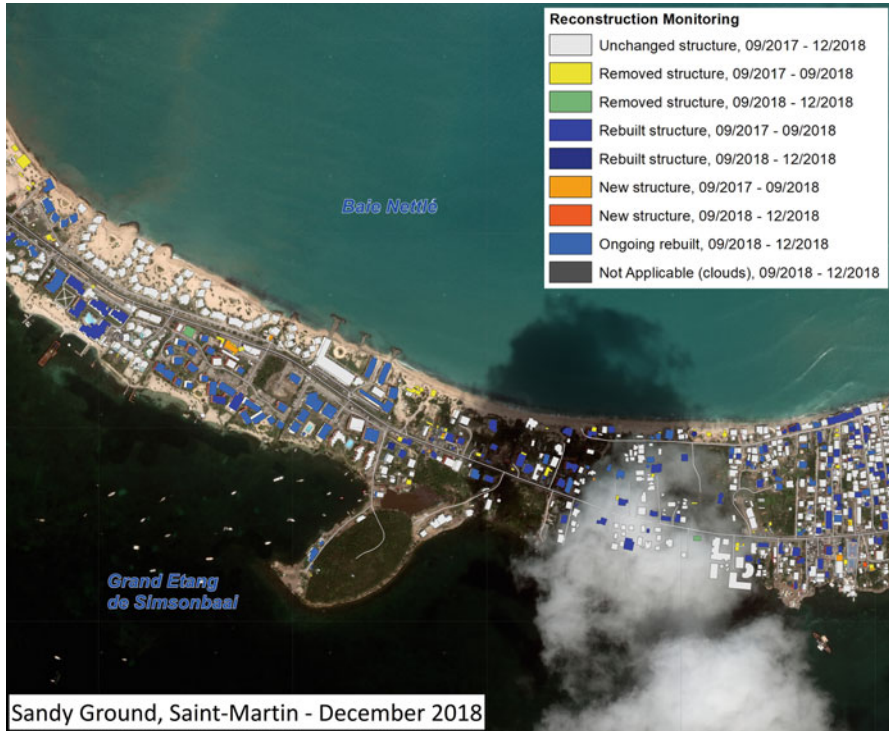


Fig. 3 Copernicus satellite-based monitoring product, St. Martin, December 2018. (Courtesy of Copernicus)



**Fig. 4** Copernicus satellite-based monitoring product, St. Martin, December 2018, Sandy Ground Close-up. (Courtesy of Copernicus)

(March 12, 2018), CNES proposed a preliminary version of the Copernicus RRM cartographic products, produced under contract to CNES in time for the meeting. A set of cartographic products analyzing the evolution of affected buildings, rubble storage areas, landfills, and shipwrecks was generated from Pleiades images, providing a dynamic dashboard, building by building, and discharge by discharge, of the evolution of the situation as seen from space. Under the Risk and Recovery Program, pre-qualified consortia bid to provide a service, and once awarded a contract, the consortium has 20 business days to provide the full suite of products.

This exhaustive dashboard of the reconstruction of the islands was presented through a set of printed large-scale maps during the fifth Inter-Ministerial Committee meeting at Matignon, the French Prime Minister's offices.

The Copernicus project has taken over since the end of March 2018 for regular cartographic production, delivered in the form of directories of vector/raster files and reports. These results made it possible to write monthly briefing notes summarizing the Copernicus results between September 2017 and July, August, and September 2018 for the Elysée (French Presidency). This work served to prepare the Council of Ministers at the end of August 2018, dealing with the post-Irma situation in the Northern Islands and the first anniversary of the hurricane, in September 2018.

Once the work of the Inter-ministerial Committee was completed, the DEAL Guadeloupe became the reference partner for Copernicus at the end of 2018, with the strong involvement of their GIS unit. The DEAL felt the collaboration with Copernicus was the only mechanism allowing unfettered access to interpreted EO data, covering the whole territory, with an almost monthly update. These Copernicus-based results were the basis for official statistics on reconstruction progress, as they were the only source of comprehensive, repeated, comparable, objective, and available statistics.

The satellite-based databases provided:

- Estimated damages to buildings evaluated within the framework of refunds from insurers, immediately after the event
- Condition of buildings during imaging periods: post-Irma (September 2017 baseline) to February 2018, from February to April 2018, from April to June 2018, and from June to September 2018

While initially this quarterly frequency seemed particularly interesting to establish indices on dates of reconstruction, after 1 year, the frequency could have been reduced given the slowness of the reconstruction with St. Martin.

The data produced by processing Copernicus RRM products have been integrated into the GEOBASE as a QGIS project so that they can be viewed by all the services of DEAL Guadeloupe via a GIS cartographic tool. The raw data is also available on the data server, so it can be reused for further studies.

One concrete example of the use of Copernicus data by the GIS DEAL service is the location of possibly illegally reconstructed buildings in St. Martin. The problem of illegal, often fragile, constructions on the Guadeloupe archipelago as well as on the island of St. Martin is significant. The damage caused by Hurricane Irma highlighted the need for preventive measures. However, it is clear that the Natural Hazard and Risk Prevention Plan (PPRN), which defines zones where building is not allowed, is not always respected.

The availability of Copernicus data has allowed DEAL Guadeloupe to more precisely detect potentially problematic areas which orient controls in the field:

- Reconstruction in the red zone of the PPRN (construction in progress or completed);
- New construction in red zones where building is forbidden.

In this respect, the results of cross-referenced data made it possible to identify some 50 constructions that were presumed to be illegal because they were reconstructed in the red zone of the PPRN. This state of affairs represents a real challenge for various services in the DEAL (urban planning, sustainable housing policy, relocation of the victims, risk management). These data have allowed DEAL to have a relatively accurate and up-to-date knowledge of a territory without the need to mobilize a large number of field agents. From experience, they know that it is easier to stop a construction site than to destroy a completed construction. Finally, in

terms of dissemination of post-Irma data: acquisition of images on both islands for the needs of DEAL 971 and all French public bodies such as the French geological institute BRGM, the biodiversity agency AFB, the forestry office ONF, the geographic institute IGN but also for the needs of the scientific community. Finally, the Ministry of Environment and CNES are working together to capitalize on feedback.

This activation demonstrates the crucial importance of satellite imagery during all phases of the risk cycle. The main benefits Copernicus Risk and Recovery brings to medium-term reconstruction monitoring include:

- Quick and frequent overview of the overall evolution of reconstruction (exhaustive, detailed);
- Figures used for Inter-ministerial Delegation for Reconstruction internal work, for information to French government, and for governmental communication (press releases, preparation of Presidential state visit, etc.).

The DEAL made the following recommendations for improvement:

- Closer links between the user and the RRM project officer, with integration of the user in the process;
- Shorter activation procedure;
- Direct link between the user and the RRM contractor, with regular user feedback;
- Operator support for technical issues encountered by the end users, depending on their technical equipment and skill level (data access, formats, GIS integration, raw images, etc.);
- Improvement of product accuracy over time: through user feedback and ground information (territorial data) potentially provided by end users;
- The Inter-ministerial Delegation would have appreciated to work in French for better expression of needs and easier interactions with the Copernicus project officer. They would recommend that national languages be used both for relations with Copernicus and its contractors and for product nomenclature, for optimal use at local level.

Thanks to satellite-based EO, St. Martin and St. Barthelemy have benefited from short- and medium-term recovery monitoring, providing an exhaustive overview of the territory that was frequently updated. Through Copernicus and Pleiades, updated geo-information of spatial origin have been regularly integrated into the geomatics repository of the authorities in charge of managing the reconstruction. Products derived from satellite imagery have increased and complemented the technical means, representations, documents, and standard information sources used by DEAL (official cartography, airborne means, drones and field photographs, administrative and technical documents of all kinds, etc.). They have been dynamically integrated into the reconstruction manager's geographic database, alongside other sources of information (Fig. 5).

The Copernicus Risk and Recovery Program was initially used mostly to analyze hazard components of risk outside the disaster period. It is only more recently that it



has been actively used to monitor recovery. The project was launched in 2012 and has had some 61 activations. A new edition of this service will start in late 2019 or early 2020 and run for 4 years. It will significantly evolve, most likely proposing a standardized, rapidly triggered, component that could be well adapted to early recovery services, which would ensure continuity in image acquisition and geo-information products, after the response phase. A portfolio of standard products dedicated to these early stages of post-crisis will be available. This would allow recovery actors to activate the risk and recovery service (providing on-demand products) with the guarantee that the immediate postcrisis situation is being monitored.

### **Copernicus EMS Early Warning: EFAS-GloFAS and EFFIS-GWIS**

Under the Copernicus Emergency Management Service (EMS)-Early Warning Component, flood and forest fire forecast and monitoring information is provided to the relevant end users through:

- The European and Global Flood Awareness Systems (EFAS and GloFAS)
- The European Forest Fire Information System (EFFIS) and the Global Wildfire Information System (GWIS)

These systems merge satellite data with relevant in situ data to generate information. While EFAS, GloFAS, EFFIS, and GWIS cover two different disaster types, they share many common in situ data requirements, including real-time and historical meteorological data and a range of geographical data sets. Flood forecasting requires access to real-time and historical river location and river flow data (hydrography and hydrology), and fire monitoring requires fuel (plant health, moisture) information.

The main flood warning system used at the European level is EFAS. It aims to deliver value-added information to the national hydrological services while at the same time providing a unique overview of actual and forecasted flood situations to the European Commission's Emergency Response Coordination Centre (ERCC). EFAS provides overview maps of flood likelihood up to 10 days in advance, as well as detailed forecasts at stations where the national services are providing real-time data. This system is in fact a comprehensive, integrated satellite and in situ network, made up of more than 30 hydrological and civil protection services. The network serves as a Copernicus EMS Rapid Mapping Service trigger for pre-tasking EO data coverage over areas that will potentially flood. Authorized users are made aware of the situation and can then trigger an activation.

On a global scale, the Global Flood Awareness System (GloFAS), jointly developed by the European Commission and the European Centre for Medium-Range Weather Forecasts (ECMWF), is a global hydrological forecast and monitoring system independent of administrative and political boundaries. This system offers a more comprehensive view of the state of the world's water cycle. It couples state-of-the-art weather forecasts with a hydrological model and, with its continental scale setup, provides downstream countries with information on upstream river conditions

as well as continental and global overviews. In this sense, GloFAS is a complementary service to the more detailed EFAS. GloFAS has produced daily flood forecasts since 2011 and monthly seasonal streamflow outlooks since November 2017. Since 2018, GloFAS is a fully operational Copernicus Emergency Management Service component.

The European Forest Fire Information System (EFFIS) provides near-real-time and historical forest and forest fire information in the European, Middle Eastern, and North African regions. Fire monitoring in EFFIS comprises the full fire cycle, providing information on pre-fire conditions (fuel) and hot spots and assessing postfire damages (burned area mapping). EFFIS was established by the European Commission in collaboration with national fire administrations and constitutes a key data source to support protection of forests against fires in the EU and neighboring countries.

The Global Wildfire Information System (GWIS) is a joint initiative of GEO and Copernicus. GWIS builds on the ongoing activities of EFFIS by combining EFFIS outputs with the Global Terrestrial Observing System (GTOS), Global Observation of Forest Cover- Global Observation of Land Dynamics (GOF-C-GOLD) Fire Implementation Team (GOF-C Fire IT), and the associated regional networks. GWIS aims to bring together existing information sources at regional and national levels in order to provide a comprehensive view and evaluation of fire regimes and fire effects at a global level.

The existence of these operational services providing constant monitoring in the flood and fire fields provides a solid link to integrate satellite-based EO in full-cycle services geared toward relevant user communities. The existence of these services has made satellite observations much more critical, as they can be viewed and analyzed in a framework familiar to end-user communities. The early warning elements have also helped gain time in acquiring crisis time data over disasters.

## **Risk and Risk Mitigation**

The discussion of the Copernicus activation for Hurricane Irma highlights the usefulness of a robust satellite-based emergency service, now available to global users, activated through the European Commission, and available free of charge. While this service now addresses the full cycle of disaster management, from early warning to recovery, it remains largely a hazard-focused service, aimed at disasters and their impact. As we will see below, satellites are now equipped to address the full range of natural hazards causing disasters. However, user-driven services are not yet exploiting on an operational basis the range of possible services to be exploited tied to risk or resilience. Risk covers not only the hazard but the exposure and the vulnerability of that exposure, where exposure is the assets that will be damaged by the hazard (e.g., population, buildings, roads, bridges, but also fields, crops, industries) and vulnerability the likelihood of damage as a factor of the characteristics of the exposed elements (e.g., population type, building material, building



height, building age, types of crops). The following section examines how satellites can contribute to each of these three components of risk.

### Hazards and Unrest

The Irma example demonstrates that satellite-based services can provide valuable warning information for hurricanes, as well as rapid damage assessment or situational awareness after an event. While not all data are integrated into operational services, there are many data streams relevant to hazards – not just hurricanes but the full range of possible hazards – and other causes of disaster such as civil unrest. The table below shows at a high level how satellite data can contribute to different hazards (Fig. 6).

The main challenge to accessing hazard data is related to understanding the source of the data, merging the data with other related data sets, and acquiring some data commercially. In some cases, there are regulatory constraints on who can access the data or where data can be collected. Most western commercial sensors cannot, for example, provide data to nationals of countries on specific lists or acquire very high-resolution near-real-time data over identified sensitive areas.

### Exposure

Until now, the entire discussion has focused on hazard. Risk, however, is not just information about hazards. Satellites can provide detailed and up-to-date information about exposure, which is a critical factor for understanding risk. Exposure is

Hazard	Main Contribution	Main Data Sources VHR : very high resolution ; HR : high resolution; SAR : synthetic aperture radar
Floods	Flood extent in near-real time	VHR/HR SAR and optical data
Windstorms	Wind and rain damage	VHR optical
Wildfires	Burned area maps, « hotspots »	Medium resolution optical, thermal
Earthquakes	Rapid damage assessment to the built environment and landslide mapping, co and post seismic displacement	VHR optical, SAR interferogram
Volcanoes	Ground displacement, ash cloud monitoring, pyroclastic flow damage, main ash deposits	SAR data stacks, low and medium resolution meteorological satellites (geo and polar orbiting optical)
Landslides	2D mud and earth movement Damage to the built environment 3D ground displacement	SAR data stacks, VHR optical
Drought	Vegetation health; long-term plant health trends	Vegetation monitoring (NDVI or other index) from low and medium resolution optical.

**Fig. 6** Satellite data applications for hazard analysis

defined as “the situation of people, infrastructure, housing, production capacities, and other tangible human assets located in hazard-prone areas.” As stated in the UNISDR glossary, “measures of exposure can include the number of people or types of assets in an area. These can be combined with the specific vulnerability and capacity of the exposed elements to any particular hazard to estimate the quantitative risks associated with that hazard in the area of interest.” In considering exposure, the usefulness of satellite data and the type of sensor to be used may vary significantly whether one is considering urban exposure (populations, buildings, networks) or rural exposure (population, crop types and values, land cover).

Detailed risk assessment requires an understanding of the impact of the hazard on built areas and other assets. In many cases, these data sets are years, if not decades, old. Very high-resolution satellite data can map at a building level or provide land-cover level assessments that place neighborhoods into a typology of affected areas. For some hazards, this work is fundamental to developing structural risk reduction measures. This is the case for slow onset flooding, for example.

Many practitioners use OpenStreetMap (OSM) as a base layer for exposure analysis, but as the example below over Jakarta demonstrates, even in areas where OSM is relatively densely populated with data, key information is often missing or misleading, and augmenting OSM with satellite data can be valuable in high-risk areas. In the example below, the first image is an OSM layer for Jakarta’s port district. The information is up-to-date and provides a high level of detail.

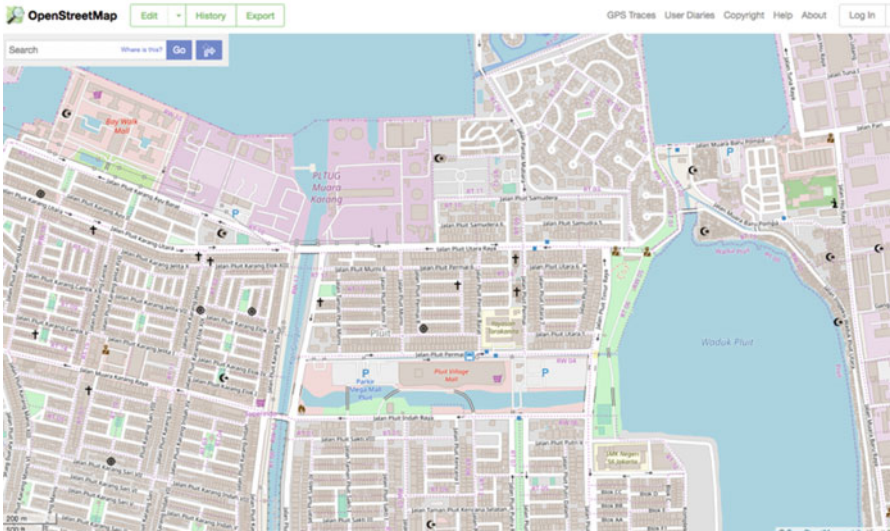
Closer examination however reveals that the information is incomplete. The image below was produced in the RASOR project ([www.rasor.eu](http://www.rasor.eu)) using a combination of OSM and detailed analysis of Pleiades satellite imagery. The imagery reveals further industrial infrastructure in the vulnerable port area. In areas where OSM is not as up-to-date, discrepancies might be much stronger (Figs. 7 and 8).

## Vulnerability

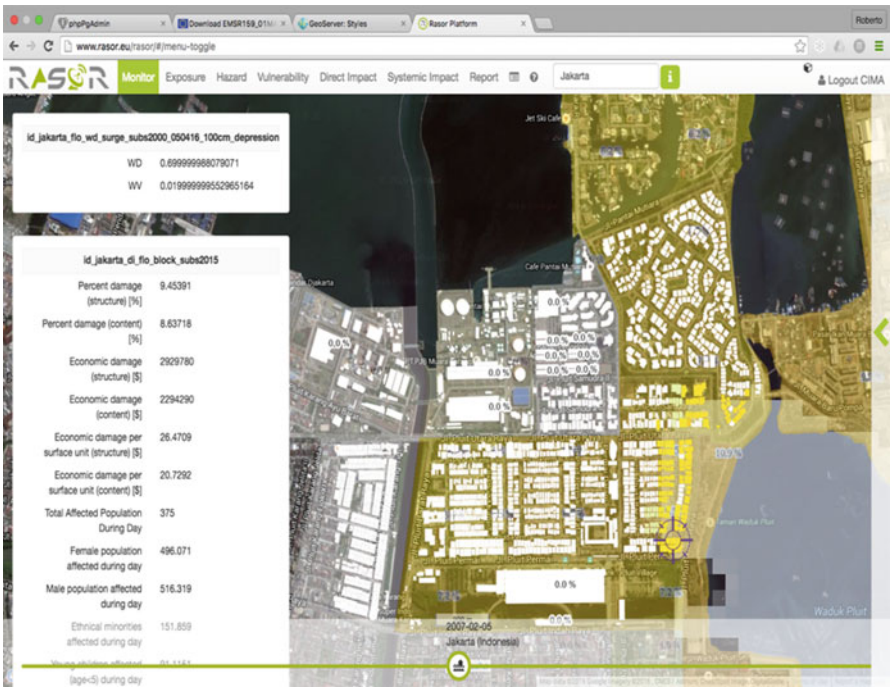
The final component of the risk analysis is vulnerability. Vulnerability is defined by the UNISDR (International Strategy for Disaster Risk reduction, now UNDRR) as “conditions determined by physical, social, economic, and environmental factors or processes, which increase the susceptibility of a community to the impact of hazards.”

Vulnerability can therefore be high or low depending on conditions, for example, people living in low-lying areas experience higher vulnerability to flooding than people who live higher up. There are different types of vulnerability, for example:

- Physical vulnerability: wooden homes which are less likely to collapse in an earthquake are more vulnerable to fire.
- Economic vulnerability: poorer families may live in squatter settlements because they cannot afford to live in safer (more expensive) areas.
- Social vulnerability: when flooding occurs some citizens, such as children, elderly, and differently able, may be unable to protect themselves or evacuate if necessary.



**Fig. 7** OSM screen capture of Jakarta port area showing infrastructure and buildings. (Courtesy of OSM)



**Fig. 8** RASOR screen capture of Jakarta port area showing infrastructure and buildings, based on merged OSM and Pleiades data. (Courtesy of RASOR)

- Environmental vulnerability: forested and deforested lands do not respond the same way to extreme weather events. Healthy ecosystems reduce environmental impacts from disasters.

There is significant overlap among these types of vulnerabilities, which is why when conducting vulnerability assessments, all these factors must be considered. However, when using satellite data to consider risk, practitioners are usually more concerned with physical vulnerability, as well as environmental vulnerability. Other types of vulnerability cannot be well measured by satellite. Indeed, traditionally, little data on vulnerability could be derived from satellites. Practitioners work with vulnerability curves developed initially in the USA such as HAZUS (GIS-based natural hazard analysis tool developed and distributed by the US Federal Emergency Management Agency). These curves are however adapted to US building types and do not export easily to Europe and even less so to developing countries. These curves must be adapted, and to adapt them, satellite information can occasionally provide useful information. This work is still not used operationally.

Understanding vulnerability is important to adopting effective risk reduction strategies, and satellite data could theoretically reduce the cost of collecting vulnerability information. In the case of both seismic and flood risk in urban areas, the structure, material and dimension of buildings, and their distance from other structures can be relevant. Understanding the plan, elevation, and structure of buildings allows the development of a building inventory which will allow a proper adaptation of the vulnerability curve to be applied to a given geographic area.

One of the most successful recent projects adapting remote-sensing data for vulnerability was the FP7 SENSUM project. SENSUM helped understand the changes in society's vulnerability and to integrate this into robust estimates of risk and of losses that follow an extreme natural event. This is especially important in countries where area-wide knowledge of the existing building stock is lacking and the urban environment is rapidly changing. SENSUM combined data from Earth Observation satellites and ground-based methods such as omnidirectional camera surveys. The methodologies developed through SENSUM demonstrate the usefulness of EO to supplement existing ground-based methods for vulnerability calculation but have not allowed a stand-alone satellite-based approach to emerge. The table below shows elements that can be derived through EO data, as proxies for in situ information, and associated vulnerability curves as modified (Fig. 9).

## **Evolving Supply and Hot Topics for Security**

### **New Satellite Missions**

The satellite world is quickly evolving. This discussion was opened by indicating that the number of EO satellites available to provide imagery for disasters, risk, and security has roughly doubled in the last decade and is poised to do so again. These missions bring more data of the types that have existed before (medium-, high-, and very high-resolution optical data, medium-, high-, and very high-resolution X, C,



**Fig. 9** EO proxies for vulnerability and resulting vulnerability curves. (Courtesy of SENSUM)

and L-band SAR data) but also new data types (S-band SAR, Ka-band SAR interferometry) and new monitoring configurations (e.g., high elliptical orbits or missions focused solely on water cover). It can be expected that these new data types will offer new applications, but the broader availability of data, and free and open data in particular, is enabling a range of new services not specifically tied to Copernicus but flowing from the data sets generated within the program. In this regard, it is worth citing the emergence of global volcano monitoring and rapid earthquake science products as two mature examples of how these data are being used.

**Data Philosophies, New Sources, and Standards/Guidelines/Best Practices**

The availability of free Copernicus data has been a major driver for the emergence of new services, such as risk monitoring. These services are user-defined and user-driven and often include new sources of complementary data that greatly increase the relevance of satellite data. Some noteworthy examples are the fusion of satellite images, drone data, and crowd-sourced information.

While drones alone can provide detailed surveys of affected areas, the use of drones in conjunction with satellites offers even more possibilities. Satellites detect affected areas, and the information can be relayed automatically to deployed drones in the zone. Drones are in fact a built-in component of the Copernicus EMS, but with

limited means, the program cannot offer a wide enough array of drones to provide comprehensive use. One project trying to better exploit these synergies through use of the Internet of Things (IoT) is the Myriad project. Myriad triggers autonomous UAV surveys based on changes detected over Copernicus imagery. Monitoring large areas with drones is usually costly. Given the scale of the area to be surveyed, important changes in the landscape can go unnoticed, which may lead to environmental and security issues. Myriad aims to solve this problem using artificial intelligence to detect changes over Copernicus data sets from Sentinel-1, Sentinel-2, and Sentinel-3, sending those changes to a UAV that will then automatically survey the change. The acquired images will be further processed to confirm or discard the detected change. The whole service will be served through an online data viewer, where the user will be able to explore those changes in real time. The Myriad project suggests that the market for drones as a service may grow to as much as \$US 18 billion by 2022.

The widespread adoption of mobile devices and social media platforms, coupled with the development of low-cost sensors, has made it easier for the public to contribute to and engage in scientific research and monitoring. This collaborative exchange with the scientific community is commonly referred to as crowdsourcing or citizen science. Numerous initiatives have emerged that actively involve citizens in environmental monitoring and stewardship, using citizen involvement to validate or complement EO data. The Group on Earth Observations (GEO) has dedicated a community activity to citizen science and lists a range of areas where citizens' observations, data, and information can complement official, traditional in situ, and remote-sensing EO data sources, including climate change, sustainable development, air quality monitoring, vector-borne disease monitoring, food security, flood, drought and natural perils' monitoring, and land cover or land-use change, among other topics. There is an enormous potential to use citizen-driven observations in combination with EO data from the Sentinel family of satellites, NASA Earth Observing Systems, and commercial imagery. Citizens provide in situ data for calibration and validation activities and for the integration of satellite and citizen observations to fill existing gaps. One of the leading applications of crowd-sourced data for disasters is Humanitarian OpenStreetMap (OSM) Team or HOT. HOT is regularly deployed during crisis situations to generate rapid situational awareness and provide a ready corollary for satellite-EO ([www.hotosm.org](http://www.hotosm.org)). Given the strong focus of HOT on exposure and vulnerability, they are an ideal complement to satellite-based hazard mapping.

The European Commission (EC) has established Citizens' Observatories that are community-centric initiatives where citizens become more active in collecting and sharing environmental information, typically harnessing the latest technological advances (e.g., ubiquitous Internet connectivity, IoT, machine learning, social media, portable and inexpensive sensors). Citizens' Observatories empower citizens to get informed and actively participate in environmental decision-making, raise awareness about environmental issues, and help build more resilient societies. The seventh Framework Programme funded five Citizens' Observatories relating to various environmental issues such as air quality, flood and water management,

coastal ecosystems, biodiversity, and odor annoyance. Horizon 2020 added four more: LandSense, Ground Truth 2.0, SCENT, and the GROW Observatory. Leveraging citizen input will enhance and augment the influence of existing Earth Observation monitoring systems, including GEOSS (Global Earth Observation System of Systems) and Copernicus.

In parallel to this, satellite data providers themselves are improving the specifications used to acquire and compile data for disaster users. Groups such as the International Working Group on Satellite-based Emergency Mapping (IWG-SEM) have drafted guidelines to set standards for the production of satellite-based maps, in an effort to ensure that satellite-based products meet clear quality thresholds to enable users to trust them.

According to the IWG-SEM Guidelines, the aim is to help support an effective exchange and harmonization of emergency mapping efforts leading to improved possibilities for cooperation among involved Emergency Mapping Organizations. This should facilitate the convergence of mapping procedures and thematic content across production teams in multiple response organizations, especially in the early response phases of disaster events. Easier information exchange allows for merging and quality checking of individual data/information layers generated by more than one Emergency Mapping Organization. The guidelines provide a framework, enabling the emergency mapping community to better cooperate during crisis times. The guidelines:

- (a) Define fundamental principles;
- (b) Establish a procedure for interactions and sharing of data, analysis, and mapping results;
- (c) Organize mapping products, templates, and dissemination policies;
- (d) Anticipate problems of uncertainty in communication;
- (e) Commit to assurance of capacity and qualification;
- (f) Prepare a glossary for emergency mapping vocabulary.

Additional separate, short, and thematically focused sub-chapters have been and are being published relating to specific disaster types.

In summary, the combination of satellite imagery, drones, and crowd-sourced data will offer a significantly more robust capability than has been available previously, supporting full-cycle risk management applications.

### **Initiatives and Services (Copernicus Security SEA)**

In terms of relatively new services and service extensions, it is worth highlighting the Copernicus Service in Support to EU External Action (SEA), which has a security mandate, as well as emerging recovery-based pilots such as the CEOS-led Haiti Recovery Observatory, and new plans for the development of generic capabilities together with the EU, the World Bank, and UNDP.

The Copernicus Service SEA aims to support European Union policies by providing information in response to Europe's security challenges. It improves crisis prevention, preparedness, and response in three key areas: border surveillance,

maritime surveillance, and support to EU External Action (SEA). Full-scale services are being developed to operationalize the use of satellites for border and maritime security. In parallel, the EU has established a service which brings satellite assets to bear for external crises when the EU seeks information to support policy decisions. As a global actor, Europe has a responsibility to promote stable conditions for human and economic development, human rights, democracy, and fundamental freedoms. In this context, the EU can provide assistance to third countries in a situation of crisis or emerging crisis and thereby help prevent global and trans-regional threats from having a destabilizing effect.

Pursuant to an agreement signed on October 6, 2016, the European Commission entrusted the European Union Satellite Centre (EU SatCen) with the SEA component of the Copernicus Security Service. In particular, the SEA component assists the EU in its operations, providing decision-makers with geo-information on remote, difficult to access areas, where security issues are at stake. It targets mainly European users, but it can also be activated by key international stakeholders, as appropriate, under EU international cooperation agreements. While still a relatively new service, the SEA security service has received positive feedback that demonstrates that the service responds to real needs, with ongoing user community enlargement.

Another example of innovative use of satellites is the Recovery Observatory effort led by CEOS with the World Bank, UNDP, and European Union. On a global scale, in both developed and developing countries, disasters strike regularly. Disasters sometimes take on monumental proportions, whether because of particularly vulnerable populations, a dramatic natural event, or exceptionally unfortunate circumstances. Hurricane Katrina, the 2010 Earthquake in Haiti, Typhoon Haiyan, or the Great Tsunami of Eastern Japan are examples of disasters that occupy a special place in our collective memories as mega-disasters after which people and governments take years to rebuild. Hurricane Matthew in Haiti was such a disaster. Since 2014, CEOS has been working on means to increase the contribution of satellite data to recovery from such major events. In December 2016, after the impact of Hurricane Matthew in Haiti became apparent, CEOS triggered the Recovery Observatory (RO). A project team made up of CEOS agencies, national partners, and international DRM stakeholders was established to oversee this project for a period of 4 years.

The aim of the RO is to:

- Demonstrate in a high-profile context the value of using satellite Earth Observations to support recovery from a major disaster:
  - Near term (e.g., support to PDNA process);
  - Medium term (e.g., recovery planning and monitoring, for up to 4 years).
- Work with the recovery community to define a sustainable vision for increased use of satellite EO;
- Establish institutional relationships between CEOS satellite data providers and stakeholders from the international recovery community;
- Foster innovation around high-technology applications to support recovery.



The main benefits of the RO include:

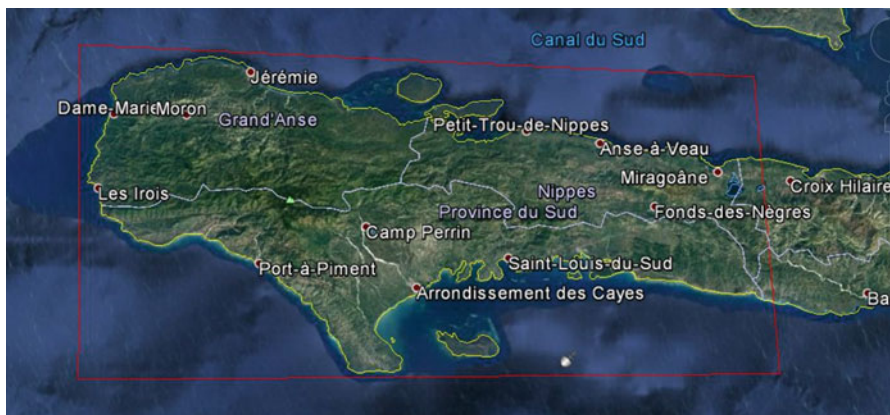
- Providing key information (analytical, geospatial) about the recovery to support end users in their decision-making processes and progress monitoring;
- Obtaining access to regular imaging of affected area over a long period, especially for higher-resolution data not typically available;
- Compiling in a single framework the key data sets (both satellite images and large number of other data) and use them seamlessly;
- Establishing a “real-life” demonstrator to identify where EO can bring useful information in the recovery phase and define “best practice” for the DRM community;
- Demonstrating usefulness of sat EO, together with other data sets, on a large scale for long-term recovery monitoring;
- Demonstrating applications tied to very high-resolution imagery and to high-frequency high-resolution images, to open the way to broader use of satellite EO after smaller events, and more regularly.

In May 2017, May 2018, and again in May 2019, the RO team made up of national champions; the French, and Italian space agencies; and international DRM stakeholders such as UNDP, World Bank/GFDRR, and EU delegation convened user workshops to bring together RO users around a list of main themes and to discuss RO products in each of these thematic areas (Fig. 10).








The table below summarizes the main thematic areas covered by the Haiti RO and the data served to develop the RO products (Fig. 11).

The RO platform is now up and running, and more data are being added regularly. It can be accessed at: <https://www.recovery-observatory.org/>

The CEOS RO partners, together with the World Bank/GFDRR, the United Nations Development Programme, and the European Union, are considering how



**Fig. 10** Haiti Recovery Observatory area of interest. (Courtesy of Google Earth and CNES)

RO : Products Thematic Table (EN) April, 2019				
	Produit	Utilisateur-clef	Elaboration	Données satellites
	Buildings Mapping	CIAT / Planning Ministry	CNES/SERTIT, Copernicus EMS R&R	Pléiades, WorldView-3
	Terrain Motion Change Detection	BME / URGeo	ASI, CNES/EOST	COSMO-SkyMed, Pléiades, Spot 6/7, TerraSAR-X
	Watershed / Flood	ONEV / Agriculture Ministry	ASI/CIMA Foundation	Pléiades, COSMO-SkyMed
	Agriculture	Agriculture Ministry	Copernicus EMS R&R	Sentinel-2, Spot 6/7, GeoEye-1, WorldView-2
	Macaya Park Monitoring	ANAP / ONEV / Environment Ministry	Copernicus EMS R&R, CNES/SERTIT	Spot 6/7
	Environmental Impact	ONEV / Environment Ministry	Copernicus EMS R&R	Sentinel-2, Spot 6/7, Pléiades, WorldView-2
	Land Use	All	CNIGS, CNES	Sentinel-2

**Fig. 11** Haiti RO thematic products. (Courtesy of CEOS, CNES, and CNIGS)

to take the lessons learned from the Haiti RO and apply them to a generic RO concept that could be activated on a regular basis after catastrophic events.

In summer 2018, the Generic RO ad hoc Development Team was established to develop possible scenarios for such a generic, scalable, and replicable observatory. They are currently developing an advocacy paper to examine lessons learned through the application of satellite data to recovery challenges.

## Conclusions

While in recent years, the application of satellite data to risk management and security issues has grown considerably and new services have emerged, there is every expectation that in the coming years, this trend is likely to accelerate. Not only are satellites more numerous than before and is satellite data more easily accessible, but the number of services integrating satellite data into operational security-related products is also growing. In Europe alone, the Copernicus program is likely to see its services augmented through a number of public good and commercial services spun off from the Horizon 2020 research program and related initiatives.

The real challenge for risk and security users is to understand the offering and identify services – or if not, data sets – that are adapted to their needs. For those integrating data into their own systems, there is a growing challenge of big data: very large data volumes required to drive new applications and the need for comprehensive processing capabilities to address these needs. In Europe, this data challenge is being addressed to some extent by the European Space Agency, which has foreseen the need for increased processing and integration capacity and has created a series of Thematic Exploitation Platforms or TEPs, many of which are directly related to security. Currently the TEPs address:

- Coastal themes;
- Forestry;

- Hydrology;
- Geohazards;
- Polar themes;
- Urban themes;
- Food security (under definition).

Similarly, new initiatives are coming forward to address clear needs. The experience in the Haiti RO is being expanded through collaboration from the World Bank, UNDP, and the EU to include a generic approach to accessing satellite-based recovery information. In the area of climate change, another new initiative, the Space Climate Observatory (SCO), aims to bring satellite data into play for situational awareness of climate impacts at the local level, offering a clear complement to global scale climate change models and observations. This new system may offer valuable data to climate-related security issues which will likely be a major theme of the next decade.

In many risk and security contexts, end users have access to classified data sources which are set up to provide a single stream of data and information. Being able to merge these classified data sources with a growing and increasingly rich set of public and commercial missions is not an insignificant challenge. In the increasingly complex network of systems and data streams, the ability to navigate, discriminate, analyze, and effectively add value will be a sought-after commodity among security users. Perhaps even more critical, the ability to do this in real or near-real time saves lives and protects property. As long as satellite data requires significant and sometimes expert human analysis, the cost of prevention and preparedness is prohibitive, and the ability to deliver in real or near-real time is illusory. The introduction of self-learning systems and other artificial intelligence in data interpretation will likely offer a major increase in mapping capacity and revolutionize the usefulness and hence the use of satellite data for risk and security in the decade to come.

---

## References

- <http://effis.jrc.ec.europa.eu>
- [http://gwis.jrc.ec.europa.eu/static/gwis\\_current\\_situation/public/index.html](http://gwis.jrc.ec.europa.eu/static/gwis_current_situation/public/index.html)
- <http://sertit.u-strasbg.fr/RMS/>
- <http://www.efas.eu>
- [http://www.eohandbook.com/eohb2015/files/CEOS\\_EOHB\\_2015\\_WCDRR.pdf](http://www.eohandbook.com/eohb2015/files/CEOS_EOHB_2015_WCDRR.pdf)
- <http://www.globalfloods.eu/>
- <http://www.hotosm.org>
- <http://www.sensum-project.eu/>
- <http://www.un-spider.org/risks-and-disasters/disaster-risk-management>
- <https://emergency.copernicus.eu/>
- [https://insitu.copernicus.eu/FactSheets/CEMS\\_Early\\_Warning](https://insitu.copernicus.eu/FactSheets/CEMS_Early_Warning)
- <https://www.copernicus-masters.com/winner/myriad-satellite-triggered-drone/>
- <https://www.pixalytics.com/eo-satellites-in-space-2018/>
- <https://www.recovery-observatory.org/>



# Space-Enabled Systems for Food Security in Africa

# 40

Olufunke Adebola and Simon Adebola

## Contents

Introduction .....	760
The Rationale for Improving System Efficiency, Integration, and Optimization .....	761
Space Technology Capabilities for Enhancing the Agriculture Value Chain .....	764
Information Generation .....	764
Information Transmission .....	765
Route Optimization .....	766
Integrated Decision Support .....	766
Challenges and Solutions to System Integration in Agriculture .....	767
Knowledge and Skills .....	767
Infrastructure Backbone .....	767
System Interoperability .....	768
End-User Interfaces .....	768
System Maintenance and Upgrades .....	769
An Example of an Integrated Agriculture Decision Support System .....	769
An Integration Model in Practice .....	772
Legal, Political, and Economic Considerations .....	773
Conclusions .....	774
References .....	776

## Abstract

Africa would be able to fulfill only about 13% of its food needs by 2050. Systemic challenges such as postharvest loss cut across the agricultural value chain and represent an opportunity for integration and optimization, with space

---

O. Adebola (✉)

Sam Nunn School of International Affairs, Georgia Institute of Technology, Atlanta, GA, USA  
e-mail: [oadebola3@gatech.edu](mailto:oadebola3@gatech.edu)

S. Adebola

Capacity Direct LLC, Atlanta, USA  
e-mail: [space@capacity-direct.com](mailto:space@capacity-direct.com)

technologies serving as a backbone for information generation, transmission, route optimization, and decision support. The chapter reviews space-based applications in support of decision-making processes of policy makers and presents a conceptual framework for their implementation in agriculture in general with postharvest loss reduction as an example.

---

## Introduction

Space technologies play an important role in modern agriculture. They are deployed to strengthen agricultural practice by increasing the effectiveness of production and optimizing the efficiency of resource allocation at each stage of the agricultural value chain. There is a global consensus captured within the Millennium Development Goals (MDGs) and the succeeding Sustainable Development Goals (SDG) to leverage all necessary means to advance the state of humanity by accomplishing defined targets for bridging the development gap within the global community. This consensus has influenced the essential role that space technologies play in economic development, and their contribution towards achieving agriculture-related targets for nutrition, health, and environmental sustainability. This consensus to which space technologies contribute, has been reinforced by the principles, policy guidance, regional coordination, and domain-focused implementation efforts executed by the various United Nations instruments and organizations, including the UN-COPUOS, UNOOSA UNOSAT, WMO, and GEO, supporting the FAO and WFP in their mandate to end hunger globally (United Nations 2015). National and regional governments have recognized the role that space technologies play in agriculture and also justify investments in their space programs based on the enhanced capabilities they provide.

The technology triad of space-based imaging, geo-navigation, and satellite telecommunications enable the significant technological advances in agriculture that drive precision agriculture and are exponentially enhanced by the technologies driving the fourth industrial revolution. These disruptive technologies include big data analytics, the internet of things, artificial intelligence (AI), cloud computing, distributed ledger technologies, AI-powered robotics, and automation. Agriculture benefits from the multiple intersections of these technologies, and their convergence with the space triad on internet-enabled digital products, applications, processes, and platforms, is driving a new wave of advancements in precision agriculture, food processing, agriculture value-chain management, and commodity trading. Although primarily tied to private sector investments (Gagliardi 2018), the ensuing competitive edge gained by the early adopters of these technologies and approaches, exacerbates existing gaps in agricultural productivity and efficiency faced by developing countries. This chapter addresses that gap by highlighting the use of integrated systems that utilize space technologies in addressing one of the major problems facing agriculture (post-harvest loss), and that poses severe consequences for low- and middle-income countries.

Post-harvest Food Loss (PHL) is defined as measurable qualitative and quantitative food loss along the supply chain, starting at the time of harvest till its

consumption or other end uses (De Lucia and Assennato 1994). It is also defined as the “losses due to spillage and degradation during handling, storage and transportation between farm and distribution (FAO 2011).” Losses can be quantitative – a reduction in the weight of edible grain or food available for human consumption. Losses could also be qualitative – reduction in weight due to factors such as spillage, consumption by pests and due to physical changes in temperature, moisture content, and chemical changes (Buzby and Hyman 2012).

Food loss has negative effects on the environment. Food in landfills decomposes anaerobically, yielding methane emissions, a gas more than 25 times as potent as carbon dioxide at trapping heat (FAO 2013). The Food and Agriculture Organization (FAO) ranks global methane emissions and places food wastage third after the United States and China. Communities affected by postharvest food losses lose out on the full benefits that agricultural products can offer in the form of nutrition, health, and wellbeing, and the use of plant products as an alternative to fossil fuels in energy generation. The use of “food” as biofuels continues to grow and may represent another demand factor adversely affected by food loss through wastage.

Agriculture is also a predominant sector of the economy and so reducing food waste could contribute to meeting the Sustainable Development Goals (SDGs). The agricultural sector accounts for 25% or more of gross domestic product (OECD and FAO 2016) and about 65% of jobs on the African continent (OECD/FAO 2016). It can be expected that a reduction in postharvest loss will increase household income and enable households to provide better education and healthcare for their families.

Global population growth could result in unmet demand for food supply which could result in political instability and unrest. This food insecurity has been blamed for protests such as those in North Africa in 2011 and the Arab Spring driven by the government’s inability to address rising caloric demands and food prices (Johnstone and Mazo 2011). In addition to this, food insecurity would also increase migration, as people seek better opportunities for food. Similarly, ongoing conflicts and insurgency situations may be driven by the ability of terrorist organizations to “win the hearts of the people” through the provision of basic needs such as food and security (Mooney and Hunt 2009).

This chapter describes findings from a technology adoption study on postharvest loss in Africa (Adebola 2020). Field research was completed in Ghana during the summer of 2019 with questionnaires administered alongside focus groups and key informant interviews with stakeholders in the agricultural sector at multiple levels. This chapter provides lessons learned from the study and describes how space-enabled technologies can play a key role in improving the agricultural value chain and help address the problem of postharvest loss.

## **The Rationale for Improving System Efficiency, Integration, and Optimization**

Solving the postharvest loss problem has long consumed the attention of actors in the engineering and development sectors. In the 1970s and 1980s, conventional wisdom

offered modernization through technology adoption as the solution to the reduction of global postharvest loss. During this period, attempts to reduce postharvest loss have adopted a “one size fits all approach.” Technologies such as improved seeds were deployed to “close the yield gap” and storage technologies were deployed to preserve the harvest. However, the effectiveness of these technology interventions has been inconclusive in Africa because of the heavy focus on the production and storage stages of food production.

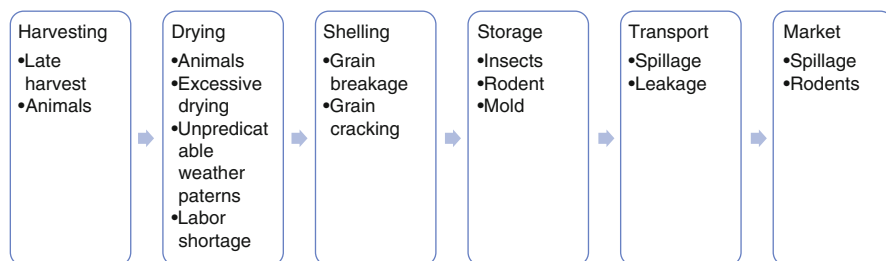
Breaking away from a silo mentality in dealing with the problem of postharvest loss at single points within the agriculture value chain, this chapter proposes a systems approach, driven by space and other technologies in addressing the problem. According to Florkowski et al. (2009), there are three advantages to adopting a systems approach. Firstly, this approach offers the opportunity of providing improvements in the continuum and allows for predicting the impact of changes along the value chain without modifying the system. Furthermore, the systems approach can identify knowledge gaps and aid in prioritizing the efforts of researchers.

Food production is not a linear process but a chain that consists of a network of interdependent stakeholders involved in growing, processing, and selling the food to consumers. This network consists of:

- Food producers such as the farmers that trade, research, cultivate the food or raise animals for meat or milk
- Food processors that provide value-added services such as food processing and butchering, produce aggregators
- Food distributors, and those that market and sell food
- Food consumers
- Food regulators, including government and nongovernment organizations that monitor and regulate the entire food value chain from producer to consumer

According to the African Postharvest Loss Information System (APHLIS), about 18% of cereal harvested in Africa is lost before it is consumed (Africa Postharvest Loss Information System 2017).

Figure 1 shows the causal agents of postharvest losses across the cereal value chain. The magnitude and pattern of maize loss vary across the food supply chain.



**Fig. 1** Causal agents of Postharvest losses across the cereal value chain. (Source: Authors)

According to APHLIS estimates, about 6% of maize grown is lost at the harvesting and drying stages. At the harvest and drying stages, too early harvest will contribute to increased moisture content, making the commodity vulnerable to mold growth and invading insects. Too late harvest exposes the crop to birds and rodent attacks, and losses caused by natural disasters. Sun-drying also exposes the commodities to pests such as birds, rodents, insects, and other domesticated animals. Often, when mechanical dryers are used, the grains are not dried efficiently, leading to broken grains (Grolleaud 2002).

The traditional practice of harvesting crops by hand, using hand-cutting tools such as sickle, knife, scythe, and cutters as adopted by many smallholder farmers in Africa, has contributed to the loss of food crops at the harvesting stage (Kumar and Kalita 2017). Often, the manpower required for manual labor is inadequate because of increasing rural-urban migration, the prevalence of HIV/AIDS, and political conflicts. This has resulted in farmers delaying harvesting and subsequently, crops are exposed to pests such as birds (Paulsen et al. 2015). Furthermore, because of inadequate drying methods, most African farmers harvest their crops at physiological maturity, that is, when the moisture content is about 20–30%. The moisture content at physiological maturity makes the crops more vulnerable to pest attacks, mold growth, and other fungal contamination (Boxall 2002). Another 4% loss occurs during the drying phase. Harvested crops are usually sun-dried in developing countries (Hodges et al. 2010). Sun-drying is limiting because it is labor-intensive and weather-dependent. Farmers reported that they could predict the timing of the rains based on their experiences. This allowed them to prepare and plan to harvest in the driest period of the month of November. However, in recent times, the rains have been unpredictable with rain falling until the end of November, thereby hindering the grains from drying properly. The unpredictability of the rainfall patterns is further exacerbated by a lack of relevant weather information for agricultural practice.

Three percent of the harvest is lost during transportation to the farm because of the long distances between rural farms and the urban markets. Very often, these countries have poor road infrastructure and farmers do not have access to mechanical transportation, and so must rely on other modes of transportation such as bicycles, animal-drawn carts, and trailers. Food crops are also lost at this stage due to heat exposure, damage from pests, and theft (Ganpat and Isaac 2015).

Inadequate storage facilities contribute to a 4% loss of maize crops (World Bank 2010). Loss at this stage occurs because aggregators and traders take advantage of information asymmetry and imperfect market conditions and offer lower prices for agricultural produce. Farmers are encouraged to store their produce until they are sure they could get a higher price. In the absence of storage systems, farmers resort to storing their grains in their homes where the grains are susceptible to exposure to moisture, mold, rodent, and insect infestation. Two percent of harvested maize is lost during threshing and shelling processes. In developing countries, threshing is done through the traditional methods of manually trampling or beating the harvested crop to detach the grains from the panicles. Grain spillage, incomplete separation of the grain from the chaff, and grain breakage due to excessive striking are some of the major reasons for losses that occur during the threshing process (Kumar and Kalita 2017).



Losses could also occur when the grain is exposed to atmospheric and biotic factors during the process.

---

## **Space Technology Capabilities for Enhancing the Agriculture Value Chain**

### **Information Generation**

At different points within the agriculture value chain, information is created by different actors that: create and supply farm inputs, prepare for and assess readiness for planting, perform seedling and planting, monitor plant and crop health (and associated risks) throughout the different phases of the planting and harvesting season, carry out postharvest activities such as drying and shelling, and provide transportation services out of farms to market and storage locations. For each of these activities, space technologies provide useful information and services (United Nations 2015). Significant investments in space technology infrastructure such as the EGNOS, Galileo, GLONASS, and GPS geonavigation programs, and leagues of earth observation satellites, underscore the crucial importance placed on access to space-enabled capabilities by national and regional governments. The use of these technologies to advance agricultural practices that rely on the information that they provide, either individually or when integrated together with other data sources, is a key part of modern agriculture, with applications ranging from precision farming to animal husbandry.

### **Remote Sensing Imagery and Environmental Data**

These are used in land allocation, land assessment, precision agriculture, monitoring weather and climatic events and patterns, and modeling to predict the effect of environmental factors on farming activities. Remote sensing also provides information on the effect of agriculture on the environment. Land use, land depletion, consumption of water resources, pollution from farm waste and effluents, and other ecological threats to pristine habitats are examples of factors that can be informed using remote sensing (United Nations 2015). Some of these factors exist at the meeting point of urbanization, agricultural land use, and environmental conservation, where a tenuous balance must be achieved between expediency and excess. This is all the more critical considering the responsibility of exploiting the environment for human uses but doing so in a responsible, equitable, and sustainable manner. Too much harm done to communities and long-term civilization has been overlooked due to the need to meet rising human demand, but it is all the more necessary that the pace and effects of agriculture on the environment be considered even as we improve our capabilities to plant and farm better using technology. Remote sensing technologies provide opportunities to track the suitability of the environment for agriculture and at the same time take a pulse of the sustainability of the environment in use (Weiss et al. 2020).

## Geonavigation

In combination with mapping (Geographic Information System) and telecommunications technologies, geo-navigation provides valuable information for precision agriculture, logistics planning, and coordination in agriculture. Geonavigation data allows the overlaying of multiple types of sensor data collected at different times, about the same location (usually on the farm), so that the data can be analyzed using GIS to derive insights that are used in decision support. Also, because agricultural produce is perishable, maintaining its freshness or an unbroken cold chain between its point of production and its final destination is necessary for maintaining its nutritional and economic value. Geonavigation provides a foundation for location-based route-optimization to minimize the time spent in transit for food that needs to be delivered fresh. When combined with distributed ledger technology, geonavigation data can be used to create a tracking and quality assurance system for fresh produce that becomes crucial for maintaining an unbroken cold chain, and securing the integrity of automatic sensor readings and food inspector direct user input on the condition of agricultural products at each transit stop across the value chain. Collecting these data over time will provide reliable data for modeling the optimal conditions and transportation routes for food and other fresh agricultural products. By combining multiple data sources and technologies, a willingness to learn from failure, and applying advanced data analytics, agricultural systems can minimize losses and increase revenue while strengthening public confidence in the quality of food production (Tian 2017). This will also expand opportunities for the just-in-time production and delivery of goods for the “fresh or minimally-processed foods” industry. This is an important development for food safety and the food industry that is dependent on geonavigation data.

Another key aspect benefitting from the use of geonavigation technologies is the use of drones in agriculture (Anderson 2014). Drones are used in farm surveillance, irrigation, spraying of agrochemicals, and security. Their main benefit is the ability to replace a human presence in carrying out these activities, while serving as a low-cost, low-maintenance alternative in remote, dangerous, or expansive locations. However, geonavigation is needed to successfully deploy and manage drone technology. Precision is often required and so there may be a need to combine satellite navigation with other location sensors to provide the ability to determine farm boundaries and limit drone activity to defined areas within the farm.

## Information Transmission

Space-enabled telecommunication is generally perceived to be useful for remote locations lacking in terrestrial network communications. This is still the case in many remote farming locations where access to telephone and broadband Internet access is still only possible via satellite telecommunications. The ability to integrate communications seamlessly across communications standards and protocols that combine space-enabled telecommunications with terrestrial network-based systems

is important in agriculture. A driver for this is that agricultural produce is moved over long distances, using different transportation modalities and an array of tracking sensors deriving information on the agricultural product, its temperature, moisture content, packaging integrity, displacement, location, and other food safety, logistics, and business variables (Dlodlo and Kalezhi 2015). Tracking information received and processed in a timely manner is important in making health, safety, and business decisions relative to agricultural produce at multiple points within the agriculture value chain. A coordination point and information management system are needed to make sense of received information and tie that back to the right business or safety decisions that must be made.

### **Route Optimization**

Finding an optimal route for the location and transportation of food and other agricultural produce is supported by space technologies such as geonavigation resources. Having accurate estimates of source and destination points, distance measures, potential routes, and navigation constraints are necessary in building a shortest path algorithm to drive logistics decision-making. Additional constraints include real time information on market prices at potential destinations and the precise timing of harvesting, processing, and transportation to the most profitable delivery point, to coincide with infrequent market days. To successfully accomplish this, logistics planning must be adept at integrating geonavigation technologies with route optimization resources, agriculture domain knowledge, and market experience. Route optimization is also used in planning the operation of farm-based machinery to achieve targeted data collection and application of farm inputs such as seeds and agrochemicals (Dlodlo and Kalezhi 2015).

### **Integrated Decision Support**

The need for an integrated decision support system is to intelligently manage and use the varied data sources that can be combined to support multiple functions within agriculture. A system of this kind will coordinate end-to-end activities at each stage of the agricultural value chain (Dengel 2013). It will combine remote sensing and mapping technology, geonavigation, and satellite telecommunications technologies within a framework designed around the business rules and business processes that drive decision-making in agriculture. This is to ensure that farmers and other stakeholders have the right information to make decisions throughout the entire agricultural value chain, with the ultimate aim to reduce losses. As an integrated system of subsystems, it will provide a template for combining information flows, feedback loops, information staging, routing, and analytics (e.g., machine learning), originating from each process-based subsystem, into a composite, semantically interoperable, and synergistic whole.

## Challenges and Solutions to System Integration in Agriculture

At the nexus of development problems and potential technology solutions, lies an opportunity to address a constellation of factors that act as forces that both shape and define the problem, as well as determine if the solution will succeed (Heeks 2005). We have seen that postharvest losses are encountered along the entire food production value chain (farm to table) and thus, Postharvest loss poses as a complex problem. Postharvest loss as a construct does not exist in isolation. It is variously influenced by the domains of agriculture, environmental sciences, transportation, commerce, and the attendant social and economic factors associated with these domains which include governance, political stability, and education. Describing these interlinkages and how distinct factors from each domain contribute to and drive the problem of postharvest loss is an aspect of its complexity that will be integrated into the conceptualization, design, development, and implementation of an integrated agricultural system of systems framework. The framework is aimed at providing decision support to aid the end-to-end functioning of the agriculture value chain. Understanding complexity enables comprehensive sense-making, problem solving, and systems-thinking which are key to defining the scope of interventions as well as guaranteeing long-term sustainability (Glouberman and Zimmerman 2002). These success factors are described below.

### Knowledge and Skills

Decision support systems are an option for addressing and bridging the wide skills and knowledge gaps between successful programs and contexts, on one hand, and those struggling with reducing postharvest losses particularly in low-income countries, on the other. The goal in creating this integrated framework would be to abide by the five rights of decision support systems, which are to provide the right information, to the right person, in the right format, through the right channel, and at the right time in the workflow (Kaushal et al. 2003). However, to achieve this goal one must contend with knowledge and skills gaps, where they exist and could pose a barrier to engaging with and embracing decision support by farmers. These include gaps in improved scientific agricultural practices, technology applications in agriculture, precision farming, the use of information technologies, language barriers, collaboration, and negotiation skills. To the extent possible, an integrated system should account for and accommodate an end-user base with broad variation in skill sets and capabilities. In addition, training and end-user support can be provided to support the system's target user base.

### Infrastructure Backbone

The right infrastructure is needed to support the operation of an integrated multi-subsystem decision support system for agriculture. The required hardware and

software for data input, storage, management, analysis, exchange, and transmission should be included in designing an appropriate technical architecture for supporting all the data, process, and service components for each subsystem, as well as the flow of information between different subsystems (Uddin et al. 2017). Accurate and detailed systems documentation is needed in order to be able to perform this integration, especially if the decision support system is not being designed and developed in-house as an end-to-end system but built as a combination of existing software products from proprietary, customized and off-the-shelf sources. Similar considerations must be made in ensuring access to telecommunications services to support the implementation, monitoring, and tracking of agricultural processes, operating using varied forms of transportation on land, air, and sea. Access to geonavigation and real-time geolocation and mapping is needed to visualize and make intelligent assessments of agricultural goods in transit. In addition, the use of cloud-based services will provide a distributed infrastructure for data storage and management, global availability and access to information, reduce latency in information transfer, and increase system redundancy. The use of accompanying data management and advanced analytics capabilities on cloud platforms can be used to enhance the value of the data and develop a system with robust decision support capabilities. These will support the movement of agricultural goods across remote rural locations all through to their final disposition at processing sites, or to urban or other rural destinations for consumption.

## **System Interoperability**

Drawing from space systems analysis and design, and Internet of Things (IoT) interoperability, the actual integration of subsystems would allow their component devices to communicate with each other using different interoperability standards and protocols (Noura et al. 2019). Specifically, data transport protocols such as TCP/IP will be used for moving data over the Internet, with options for securing data transfer implemented. Data formats for data exchange would include raw data and flat formats as well as structured formats such as JSON and XML for directly ingesting data into machines for analysis and automated decision-making. Application Programming Interfaces (APIs) will support data calls and responses between different subsystems. The use of an API-centric Service Oriented Architecture (SOA) for data exchange will permit the scalability and management of interoperability features across the system.

## **End-User Interfaces**

An IoT-dense system that combines sensor data with other sources including space-enabled data, and exchanges these through APIs and an array of widgets and connectors designed to handle interoperability issues, will rely on a cross-platform web interface for deploying data visualization, information, and analytics insights

(Khattab et al. 2016). Similarly, enabling interaction with the system will support modalities such as key input, touch, voice, and motion detection. An interface, for example, should be intuitive, easy to interact with, support multiple languages, be accessible on different web-enabled devices, and have the resources for user training and support. Developing and deploying the end-user facing interfaces for the system should be done collaboratively with the end-users, system administrators, and product owners. This is to help gather their functional requirements that will then feed into the interface design, and subsequent product and user acceptance testing prior to deploying into production.

## **System Maintenance and Upgrades**

Providing and maintaining good quality service for a system in production (operational use) requires budgeting for and providing resources to support regular system maintenance and upgrades. This should cover software version upgrades and patches, as well as repairs and replacement of failed hardware. A tracking system for reported failures and outages should be in place. The advantage of a sensor/IoT-dense system is the ability to collect data that can be used to automate issue reporting and tracking, as well as the predictive modeling of system failures, in order to enable intelligent system maintenance (Chuang et al. 2019). Regular feedback and iterative design sessions can be held with stakeholders, to ensure that the system as a whole continues to deliver useful information and updated services needed to remain effective and competitive.

---

## **An Example of an Integrated Agriculture Decision Support System**

Examples have relied on combining inputs, models, feedback loops, and ensembles (Dengel 2013). This framework outlines the statistical, machine learning, and system automation approaches that will combine to integrate the varied inputs and separate models, into a functional system that captures the dependencies within the entire system. The level of description here simultaneously seeks to balance complexity with clarity in describing this integrated system (Table 1).

As described earlier, this is an IoT-dense system that combines sensor data with other sources including space-enabled data, and exchanges these through APIs and an array of widgets and connectors. The flow of information through the system is mediated through the different subsystems that manage the processes at each stage of the value chain, namely, planting, harvesting, processing (shelling, drying, packaging), storage, transportation, and market. The table above takes an integrated approach in giving examples of the different data elements, data types, and decision points relevant to each of these stages.

The flow of information seeks to enhance processes at each stage by making available information from a preceding or subsequent stage. These do not have to be

**Table 1** Examples of variation in agriculture value chain data and integrated decision support algorithms

Capability	Data source	Agricultural value chain example data set (Postharvest loss example)
Sensing/imagery	Camera	Pest control, conflict hazards, type of crop, size of farm, estimating goods volume
	LiDAR/Radar	Precipitation, flooding, pollution, hydrologics
	Hyperspectral	Leaf color, NDVI, crop health, bush fires, soil temperature, air temperature, humidity
	Sensors	Grain moisture, aflatoxin and growth, infestation, contamination, packaging integrity
Geo-location	Localization	Storage and distribution infrastructure, market access
	Geonavigation	Planting and harvesting optimization, mixed crop harvesting, transportation
	Geo-optimization	Transportation, postharvest loss minimization, automated machinery
Telecommunication	Device	Bluetooth, infrared, NFC
	Network	TCP/IP, GSM, LTE, satellite communications
	Systems	RESTful APIs
System integration	Technical	Cost minimization, system logs
	Situational	Market regulations, supply conditions (i.e., competition), transaction costs
	Environment	Governance structure, regulatory compliance
Decision support	Product	Feedback from wholesalers and retailers, crop selection, future planting, crop rotation and substitution, production decision
	Logistics	Postharvest loss optimization
	Market/pricing	Profitability, expected return on investment, market forecasting, dynamic pricing

contiguous stages for shared information to be relevant or useful. The ability of an integrated system to store historical data for analysis endows the capability of providing both real-time data and historical insights as inputs to a decision-making process. Information about provisioning and procurement of resources for a downstream process would thus benefit from estimates and current data on the volume of produce to be anticipated from single or multiple farming locations. Similarly, the timing of harvesting (an upstream process) is informed by historical data on peak pricing, other market data, and the availability of transportation options for fresh produce. An exhaustive list of bidirectional information flows and the agricultural processes that they have the potential to inform will be determined over the course of interactions with stakeholders during the design phase of the system.

With the availability of historical data and real-time data, as well as a clear definition of agricultural processes that benefit from the availability of the data, statistical methods can be applied to develop diagnostic, predictive, and prescriptive models using these data. Understanding the details of the modeled agricultural processes is a prerequisite to successfully applying statistical machine learning in

agriculture. Systems that collect, store, manage, and allow analysis, visualization, and integration of agricultural data inputs are essential for advancing the role of data as an agricultural resource, input, and asset. When machine learning models are stable in production and are successfully delivering gains in process improvements, they can then be allowed to drive agricultural process automation and inform process reengineering, where necessary. For example, the release of inventory stocks of raw produce into a food processing line based on forecasted demand to allow just-in-time delivery within the supply chain is a process that can be automated based on the success of machine learning models that draw on historical time-series data on demand patterns, as well as real time monitoring data on raw produce stocks in storage, and logistics data on transportation availability for the delivery of fresh products.

Similarly, a model for the pricing of goods at the market will need to input historical pricing data, demand forecasts, market competition data, real time inventory data, forecasts of anticipated commodity supplies, space-enabled environmental data predicting agricultural productivity, and industry financial targets, in determining where to set the price points. With additional learning, such a pricing model, that relies on the outputs of other statistical models with variable inbuilt uncertainty calculations and reliability, can be further enhanced through using artificial intelligence-based ensembles that can account for this wide variability and complexity. In addition, the pricing model can be further enhanced to maximize profit and minimize losses by varying the prices based on data on the location and timing of the sale, through using an optimization model for the setting of prices. This can then be automated as an AI-powered pricing system ensuring profitability even in the face of uncertainty which is a major factor in agricultural market risk modeling.

Agriculture is frequently described as a risky enterprise. With AI providing a way to intelligently deal with this uncertainty, a farmer can have at his disposal the tools he needs to minimize his risk in participating in farming. The same applies at every step of the value chain where actors in the agricultural value chain struggle with multiple points of failure in procuring, processing, and delivering to market various food products with different storage and processing requirements, within a highly regulated industry with stringent quality standards. AI will not eliminate all the risk in agriculture, but by linking and integrating varied data sources, and consistently doing this the right way over a long period of time, we will revolutionize the agricultural industry with significant impact on food production and availability, agriculture financing, commodity pricing, sustainable agriculture, nutrition, and hunger.

The planning and coordination of the integrated system will require skills in networked infrastructure to include the provisioning of hardware, networking, and software solutions for both back-end (resource management) and front-end (end-user facing) functions. User interface design and visual analytics skill sets will also be needed. Process automation, machine learning, optimization, and other advanced analytics skill sets will be required to turn the space-enabled and other data types into useful insights and intelligence for decision-making. Training, communications, and operational support resources are essential for successful deployment.



## An Integration Model in Practice

Data governance should not be an afterthought when building complex systems, especially those derived from multiple sources, and those that may contain regulated data such as personally identifiable information (PII). Clear and detailed rules should be outlined to govern data storage, security, access, retention, sharing, and usage. Data has inherent value and so the ownership rights to the data should also be clear before, during, and after it passes through the system. It may be necessary to constitute a group that will be responsible for monitoring, managing, enforcing, and updating the data governance stipulations for the system.

In order to understand the complexity and depth of an integrated system for an agricultural problem, it is required to exhaustively explore and comprehensively describe the current state of data collection and knowledge management systems for tracking postharvest losses. Multiple data collection methods are needed to gather the needed data from the broad end-user base which will include individual farmers, their collectives (usually farmer cooperatives), food processing and transportation service providers, government, communities and other stakeholders including external donors, and agricultural technology manufacturers and vendors. The elicited findings will be used to illustrate cases that will inform functional requirements for how the conceptual framework will work in various process scenarios. In other words, their recommendations will be tailored to contextual circumstances. This will seek to analyze how efficiencies can be gained by implementing a context-sensitive and framework-based approach. This differs from current approaches that assume that one technological shoe fits all. A framework in addition to providing a template to compile lessons learned, also enables integrating data sources into meaningful information that can then be organized to provide decision support across the value chain. After exhaustively defining the data elements that feed into and that can be derived from the food distribution and postharvest loss across the food value chain, each data element is then further described in relation to the subsystems it supports, and how it is linked to other aspects of the system. This creates an understanding of how information flows within the existing system, and how this may be optimized to work better in an integrated decision support system.

When there is a high volume of information resources, information overload (with abundant false positives drowning out the actionable signal with unnecessary noise) could become a problem. To combat this, systems must be configured and trained to detect useful information and exclude unnecessary data. AI is a powerful tool for better defining the statistical boundary on which data classification is based, in order to improve the quality of actionable information. The goal is to work with only useful data and keep data products useful and relevant to the stakeholder and end-user base.

Another goal of this framework is to ensure that implementations of the integrated system result in intelligent systems with the ability to update and optimize decision support recommendations in response to changes in the data and other environmental factors. To the extent possible, it is also desirable that implementations carry a certain level of automation to further abstract their use from the inherent skills and

expertise of the user. The ensuing postharvest loss optimized integrated decision support system (POIDS) will integrate different forms of data from a wide variety of sources, continuously streaming in, and optimize and learn from these data to automatically deliver value efficiently. This could serve as a framework for examining how a broad range of possible data elements representing widely varying upstream and downstream factors can be combined to achieve an advanced system of efficiency for agricultural and food distribution.

---

## **Legal, Political, and Economic Considerations**

The success of the system will depend on the availability and sharing of satellite data. While Article 1 of the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, Including the Moon and Other Celestial Bodies, states that “the exploration and use of outer space, including the Moon and other celestial bodies, shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development, and shall be the province of all mankind.” The concept of benefit of all has continued to be ambiguous and a subject of legal contention (Aganaba-Jeanty 2015) particularly with relation to sharing satellite data. Also, being a soft law, the Treaty does not have the force of law, as such, States can decide the interpretation of common benefit it pleases and as such can decide not to share information for reasons such as national security. It appears that the wordings of The UNGA’s 1996 Benefits Declaration that “States are free to determine all aspects of their participation in international cooperation in the exploration and use of outer space on an equitable and mutually acceptable basis” leave States to determine the extent and definition of international collaboration.

There is an obvious lack of agreement on the magnitude of the postharvest loss problem, even among highly resourced custodians of the problem in international development. Without a doubt, national governments have a role to play in the creation and validity of postharvest loss data. They, however, also face several significant challenges to meeting their governance obligations. Addressing the data availability and accuracy challenge would strengthen predictive models and better support decision-making to drive improvements along the food and agricultural value chain, to ultimately help reduce postharvest loss.

Investing in space technologies would have financial implications on the demand and supply sides. For example, on the demand side, there will be costs on the farmer for subscribing to the integrated support system service as they access information at the planting, harvesting, drying, and transportation stages. On the supply side, there are costs on the entity providing the integrated service for purchasing space data from private entities in developed countries and other sunk costs such as those of training the farmers on the most efficient utilization of the information provided and costs of business registration. It is expected that these costs will be shared among the stakeholders in the value chain. While the costs may be high in the early stages of the

deployment, it is expected that over time, the service will reach economies of scale as more farmers subscribe to the service.

---

## Conclusions

This chapter highlights lessons learned in addressing an agricultural problem that affects food security. It stresses the role of user communities in developing fitting solutions to user-defined problems while leveraging space-enabled technologies and other technology solutions.

An environmental scan of influencing factors in determining the success of integrated systems in agriculture would identify the different stakeholders, and their primary domains of interest in approaching the problem. The postharvest loss problem can be viewed as both a technology-focused or a development-focused problem. Each approach, to varying degrees, has been adopted as prevailing wisdom for resolving postharvest loss. It is, however, necessary to compare how the potential range of technology interventions have variously contributed to the success and in some cases the failure of programs aimed at improving postharvest loss. Research conducted by the authors in Ghana highlighted some issues of concern and core domains of interest as important to consider when integrating technology solutions into development programs.

African agriculture is often characterized by the low rates of adoption of Green Revolution technologies – such as high yielding crop-varieties; irrigation; and micronutrient fertilizers (Feder and Savastano 2017). Inappropriate land tenure, patriarchy, and ineffective government regulation of land use have been attributed as the cause of small land ownership in the continent (Melesse 2018). Small land ownership is broadly described as farmers farming on less than ten hectares of farmland (Samberg et al. 2016). Smallholder farmers are often described based on their resources using terms such as “small-scale,” “resource-poor,” and sometimes “peasant farmer” (Gininda et al. 2014). In effect, because of resource constraints, smallholder farming discourages farmers from investing in expensive technologies because the farms are not large enough to produce large outputs (Jayne et al. 2010).

It was observed that when acquisition costs for farmers and other stakeholders are too high then the adoption of new technological approaches will remain low (Kuehne et al. 2017). This is exacerbated by the gaps in purchasing power between the farmers on one hand, and those developing and producing the technology solutions that will be used for agriculture on the other. Similarly, access to maintenance services and the cost of maintenance, where available, could also pose a barrier to integrating technology solutions in an agricultural development program. An alternative solution to the acquisition and maintenance challenges would be the development of technologies and services locally and at a cost that will be affordable to a larger portion of the agricultural end-user base. Observations from the Ghana study show that locally produced technology is both feasible and available in practice but is prone to failure due to poor scalability where there is a lack of government or investor funding support.

Specifically, the use of space-enabled technologies has been on the increase, including among African countries, with Ethiopia recently joining South Africa, Egypt, Nigeria, Ghana, Morocco, Algeria, Kenya, Angola, and Rwanda on the list of African countries with space-based remote sensing or telecommunications assets. This should eventually lead to greater adoption of space-enabled services for agricultural purposes such as in reducing food loss, through the development and deployment of targeted, locally sensitive and context-specific solutions that embrace the challenges of their environment and provide options for disadvantaged farmers. Another option that has been tried is the provision of technologies at no cost to the farmers or their communities either through development grants or donor agency funding. It was observed that this often did not translate to immediate access for all those in need of the technology since such “gifts” still suffered from issues such as preferential allocation based on political affiliation, lack of skilled users, poor or absent maintenance, or inadequacy in meeting the need due to an insufficiently available number of the resource.

A potential approach would be to implement the concept of shared ownership of a technology resource. Ownership seeks to actively engage all stakeholders in the conceptualization, framing, and solution design of a shared problem. This allows a participatory approach, and a common sense of commitment to the success of the technology intervention. It also embraces a shared definition of success for the technology program which then allows each stakeholder to be represented in the allocation of resources relative to the intervention. The key then to increasing the adoption of an integrated system is the ability to demonstrate to farmers, at varying scales of farm size and technology advancement, how participation in the use of information technologies and taking advantage of decision support systems can enhance their farming knowledge and skills, increase their output, and profit them economically.

To further support the success of space-enabled technology interventions, the transfer of knowledge and skills to local product owners, system administrators, and end-users will serve to increase the long-term viability and sustainability of the programs. There needs to be a plan for not just immediate use of an application but also for significant technology leaps that will enable local ownership. This would solve the problem of technology interventions being abruptly disrupted due to cessation of development funding or the unexpected departure of a key resource that is difficult to replace. A previously deployed agriculture decision support tool, for precision farming and pricing, that was discontinued led to a distrust of such solutions by the farmers, and this may make it harder to convince them to adopt similar solutions in the future, especially if a cheaper alternative has been discovered. This could have been avoided if the technology intervention was deployed in a robust manner, with sufficient redundancy built into the system from a resource standpoint. It was observed that in some cases, the lack of knowledge was considered a problem at a communal level. To respond to this need, knowledge transfer can be done at a group level, over multiple iterations to ensure that knowledge stays fresh and practical. The integration of knowledge sharing platforms can further enhance access to information while providing peer support for troubleshooting and issue resolution.

Technology adoption does not happen instantly (Hall and Khan 2003). Rather, it is a process whereby some people are more willing and able to adopt innovation than others. The distribution of the actors within technology adoption models shows a bell curve where the spread of technology starts off slowly during the incubation period, accelerates during a period of rapid acceptance, and levels off as more people adopt the technologies (Caselli and Coleman 2001). Cultural factors remain a key driver of adoption and in determining if the impact will be realized from investments made in introducing technologies for development aims.

The chapter recommends pulling together varied data sources and integrating them into accessible decision support systems. These systems provide information for intelligent decision-making at the different intervention and leverage points across the agriculture value chain. Accuracy shall be refined in and through practice, and the systems should be set up to integrate new data sources, assumptions, constraints, and statistical models.

---

## References

- Adebola O (2020) Market-based approaches for postharvest loss reduction. PhD. Atlanta: Georgia Institute of Technology
- Africa Postharvest Loss Information System (2017) APHLIS+. [online] Available at: <https://www.aphlis.net/en/page/1/crop-tables#/datatables/crops-losses?metric=prc&year=2016>. Accessed 10 Jan 2020
- Aganaba-Jeanty T (2015) Common benefit from a perspective of “non-traditional partners”: a proposed agenda to address the status quo in global space governance. *Acta Astronaut* 117:172–183
- Anderson C (2014) How drones came to your local farm. [online] MIT Technology Review. Available at: <https://www.technologyreview.com/s/526491/agricultural-drones/>. Accessed 6 Mar 2020
- Bharati P, Chaudhury A (2006) Studying the current status of technology adoption. *Commun ACM* 49(10):88–93
- Boxall RA (2002) Storage losses. In: Golob P, Farrell G, Orchard JE (eds) *Crop post-harvest: science and technology volume 1: principles and practice*. Blackwell Sciences, Ltd., Oxford, pp 143–169
- Buzby JC, Hyman J (2012) Total and per capita value of food loss in the United States. *Food Policy* 37(5):561–570
- Caselli F, Coleman WJ (2001) Cross-country technology diffusion: the case of computers. *Am Econ Rev* 91(2):328–335
- Chuang S, Sahoo N, Lin H, Chang Y (2019) Predictive maintenance with sensor data analytics on a raspberry pi-based experimental platform. *Sensors* 19(18):3884
- De Lucia M, Assenato D (1994) *Agricultural Engineering in Development: Post-harvest Operations and Management of Foodgrains*. FAO Agricultural Services Bulletin No. 93. Rome: FAO
- Dengel A (2013) Special issue on artificial intelligence in agriculture. *Künstl Intell* 27(4):309–311
- Dlodlo N, Kalezhi J (2015) The internet of things in agriculture for sustainable rural development. In: 2015 international conference on emerging trends in networks and computer communications (ETNCC). Windhoek: IEEE, pp 13–18
- FAO (2013) *The food wastage footprint*. FAO, Rome

- Feder G, Savastano S (2017) Modern agricultural technology adoption in sub-Saharan Africa: A four-country analysis. In *Agriculture and Rural Development in a Globalizing World* (pp. 11–25). London: Routledge
- Florkowski WJ, Prussia SE, Shewfelt RL, Brueckner B (eds) (2009) *Postharvest handling: a systems approach*. Amsterdam: Academic Press
- Food and Agriculture Organization (2011) *Global food losses and food waste: extent, causes, and prevention*. Rome: FAO
- Gagliardi N (2018) How self-driving tractors, AI, and precision agriculture will save us from the impending food crisis. [online] TechRepublic. Available at: <https://www.techrepublic.com/article/how-self-driving-tractors-ai-and-precision-agriculture-will-save-us-from-the-impending-food-crisis/>. Accessed 6 Mar 2020
- Ganpat W, Isaac W (2015) Impacts of climate change on food security in small island developing states. Information Science Reference, an imprint of IGI Global, Hershey
- Gininda PS, Antwi MA, Oladele OI (2014) Smallholder sugarcane farmers' perception of the effect of micro agricultural finance institution of South Africa on livelihood outcomes in Nkomazi local municipality, Mpumalanga Province. *Mediterr J Soc Sci* 5(27 P2):1032
- Glouberman S, Zimmerman B (2002) Complicated and complex systems: what would successful reform of medicare look like? Commission on the Future of Health Care in Canada, Ottawa. Available from <http://publications.gc.ca/collections/Collection/CP32-79-8-2002E.pdf>
- Grolleaud M (2002) Post-harvest losses: discovering the full story. Overview of the phenomenon of losses during the post-harvest system. FAO, Agro Industries and Post-Harvest Management Service, Rome
- Hall BH, Khan B (2003) *Adoption of new technology* (no. w9730). Cambridge: National Bureau of Economic Research
- Heeks R (2005) *Implementing and managing e-government: an international text*. Los Angeles: Sage
- Hodges R, Buzby J, Bennett B (2010) Postharvest losses and waste in developed and less developed countries: opportunities to improve resource use. *J Agric Sci* 149(S1):37–45. <https://doi.org/10.1017/s0021859610000936>
- Jayne TS, Mather D, Mghenyi E (2010) Principal challenges confronting smallholder agriculture in sub-Saharan Africa. *World Dev* 38(10):1384–1398
- Johnstone S, Mazo J (2011) Global warming and the Arab spring. *Survival* 53(2):11–17
- Kaushal R, Shojania KG, Bates DW (2003) Effects of computerized physician order entry and clinical decision support systems on medication safety: a systematic review. *Arch Intern Med* 163(12):1409–1416
- Khattab A, Abdelgawad A, Yelmarthi K (2016) Design and implementation of a cloud-based IoT scheme for precision agriculture. In: 2016 28th international conference on microelectronics (ICM). Giza: IEEE, pp 201–204
- Kuehne G, Llewellyn R, Pannell DJ, Wilkinson R, Dolling P, Ouzman J, Ewing M (2017) Predicting farmer uptake of new agricultural practices: a tool for research, extension and policy. *Agric Syst* 156:115–125
- Kumar D, Kalita P (2017) Reducing postharvest losses during storage of grain crops to strengthen food security in developing countries. *Foods* 6(1):8. <https://doi.org/10.3390/foods6010008>
- Mesesse B (2018) A review on factors affecting adoption of agricultural new technologies in Ethiopia. *J Agric Sci Food Res* 9(3):1–4
- Mooney PH, Hunt SA (2009) Food security: the elaboration of contested claims to a consensus frame. *Rural Sociol* 74(4):469–497
- Noura M, Atiquzzaman M, Gaedke M (2019) Interoperability in internet of things: taxonomies and open challenges. *Mob Netw Appl* 24(3):796–809
- OECD/FAO (2016) *OECD-FAO agricultural outlook 2016–2025*. OECD Publishing, Paris. [https://doi.org/10.1787/agr\\_outlook-2016-en](https://doi.org/10.1787/agr_outlook-2016-en)
- Paulsen MR, Kalita PK, Rausch KD (2015) Postharvest losses due to harvesting operations in developing countries: a review. In: *American society of agricultural and biological engineers*

- annual international meeting 2015, vol 1. New Orleans: American Society of Agricultural and Biological Engineers, pp 562–596
- Samberg LH, Gerber JS, Ramankutty N, Herrero M, West PC (2016) Subnational distribution of average farm size and smallholder contributions to global food production. *Environ Res Lett* 11 (12):124010
- Tian F (2017) A supply chain traceability system for food safety based on HACCP, blockchain & internet of things. In: 2017 international conference on service systems and service management. Dalian: IEEE, pp 1–6
- Uddin MA, Mansour A, Le Jeune D, Aggoune EHM (2017) Agriculture internet of things: AG-IoT. In: 2017 27th international telecommunication networks and applications conference (ITNAC). Melbourne: IEEE, pp 1–6
- United Nations (2015) Space for agriculture development and food security. [online]. United Nations Office at Vienna, Vienna. Available at: [https://www.unoosa.org/res/oosadoc/data/documents/2016/stspace/stspace69\\_0\\_html/st\\_space\\_69E.pdf](https://www.unoosa.org/res/oosadoc/data/documents/2016/stspace/stspace69_0_html/st_space_69E.pdf). Accessed 6 Mar 2020
- Weiss M, Jacob F, Duveiller G (2020) Remote sensing for agricultural applications: a meta-review. *Remote Sens Environ* 236:111402
- World Bank (2010) Missing food: the case of postharvest grain losses in sub-Saharan Africa. World Bank: Washington, DC



# Satellite Communication for Security and Defense

# 41

Holger Lueschow and Roberto Pelaez

## Contents

Introduction - Historical Evolution .....	780
SATCOM Frequency Bands and Orbits .....	782
SATCOM for Military .....	784
Commercial SATCOM (COMSATCOM) .....	784
Military SATCOM (MILSATCOM) .....	784
Governmental SATCOM (GOVSATCOM) .....	784
Operational Needs .....	785
Use Cases and Applications .....	786
Military SATCOM Solutions and Systems .....	787
United States .....	787
United Kingdom .....	788
France .....	788
Germany .....	789
Italy .....	789
Spain .....	790
Luxemburg .....	790
Other European Activities .....	791
NATO .....	792
Russia .....	792
China .....	793
SATCOM for Security .....	793
European Union (EU) .....	793
European Space Agency (ESA) .....	794
Conclusion, Outlook and Perspectives .....	795
References .....	796

H. Lueschow (✉) · R. Pelaez

European Defence Agency (EDA), Brussels, Belgium

e-mail: [Holger.LUESCHOW@eda.europa.eu](mailto:Holger.LUESCHOW@eda.europa.eu); [Roberto.PELAEZ@eda.europa.eu](mailto:Roberto.PELAEZ@eda.europa.eu)



---

**Abstract**

The contents reported in this chapter reflect the opinions of the authors and do not necessarily reflect the opinions of the respective Agency/Institutions.

Today, coalition and national military operations are inconceivable without the support of space-based systems. Space-based assets and applications are essential to navigation; communication; meteorological, geospatial, and imagery services; early warning; and ballistic missile interception. They are a vital enabler for command and control (C2) and situational awareness through the provision of intelligence, surveillance, and reconnaissance (ISR) information.

Satellite communications play an indispensable role in security and defense-related governmental communication. They are used when other ground-based means of communication are not possible, reliable, or available. Satellite communications are critical assets in the ability of States to respond autonomously and in a timely manner to global defense, security, and humanitarian and emergency challenges.

---

**Introduction - Historical Evolution**

Communications have been critical to military organizations for centuries.

The year 1957 marks the beginning of the space age with the Russian SPUTNIK-1 being the first artificial satellite to go around the Earth. In 1962, the world's first active communications satellite Telstar 1 was launched. This satellite was built by AT&T and Bell Laboratories, USA. During its 7 months in operation, Telstar 1 provided to the world live images of sports, entertainment, and news. It was a simple single-transponder low-earth-orbit (LEO) satellite, but its technology of receiving radio signals from the ground, and then amplifying and retransmitting them over a large portion of the earth's surface, set the standard for all communications satellites that followed.

Since then the use of space has expanded constantly based on ever-growing demand for different types of space services, and SATCOM systems support a wide range of fixed and mobile telephone and data services including broadcast services. These are known under their official ITU definitions as the Fixed Satellite Services (FSS), the Broadcast Satellite Services (BSS), and the Mobile Satellite Services (MSS) for aeronautical, maritime, and land mobile applications. Over the years, a global change in telecommunications regulation and transition from monopolist communication providers to an open market has led to constant innovation and more competitive systems also in the satellite world.

During the 1960s and 1970s, satellite performances advanced quickly and a global commercial SATCOM industry began to develop. Focus in commercial SATCOM was for decades to support international and long-haul telephone traffic and to distribute broadcasting programs, and for many years, satellite broadcasting was the driver for the evolution of commercial SATCOM systems. Since those early days of SATCOM, commercial solutions have become more capable and could

support higher data rates and more and more services. In parallel to this evolution, the user terminals have become smaller, cheaper, and easier to operate.

This development went hand in hand with the increased sophistication of military forces. Consequently, the opportunities offered by satellites for all types of military applications including communications have been understood, and it was natural that the military explored space to receive support to meet their communications requirements. This was the baseline for SATCOM as a vital enabler to support defense-related services.

Military organizations around the world began to look at ways how to use satellites to provide communications to their forces. Starting with the U.S. Department of Defense and its Initial Defense Satellite Communication System (IDSCS – a series of LEO satellites in a random orbit constellation that allowed for more or less global communications, although there were some periodic service interruptions due to gaps in the satellite coverage), a wide range of military communications satellites have been launched by a number of other defense forces around the world in the years and decades that followed. Over the last 60 years, a variety of satellites, deployed into different orbits, have been developed by many nations to meet their governments' and particular military communication needs.

As SATCOM systems come along with high costs and long planning and realization times, most of those military SATCOM projects and initiatives cannot meet all the communication requirements the military have, be it from a bandwidth or coverage perspective. Therefore, defense forces around the world have to rely on commercial SATCOM systems. Depending on the use case and application, the support by commercial satellite capabilities has always been necessary, especially when specific needs arise or military demand exceeds available military capacities.

Today, industry has a long experience in meeting the military user demands for telephone, data, networking, audio, and video services. SATCOM services and applications form the largest space market sector and are sold on a “global open market.” Commercial SATCOM capacity is usually delivered by satellite operators who own a fleet of satellites which they procure, launch, and operate. Several different contract approaches have been used to obtain defense-related SATCOM capacity, and a whole industry has been developed around providing communications requirements for military purposes. In some cases, industry has provided the military user with full end-to-end (sometimes known as turn-key) services including the capacity leased from a commercial provider, terminals, other hardware, and operation of the full service to supplement the military capacity.

With the “new Space” and in particular the entry of new business actors from the “digital economy,” the SATCOM market was faced with considerable changes and had to react to new requirements that currently lead to new or modified business models and SATCOM services.

High-throughput (HTS) and very high-throughput satellites (VHTS) as well as new mega-constellations of satellites represent the latest technology trends and promise for the future communications support for live video with low latency and at less cost compared to a decade ago.

## SATCOM Frequency Bands and Orbits

From their initial stages, SATCOM services have quickly evolved to meet both civilian and military communication needs. The real drivers of this evolution were intercontinental and regional communication during the 1970s and the 1980s, broadcasts services, mainly TV, since the 1990s, and more recently multimedia applications.

An efficient management of the limited and scarce resource of frequency spectrum as well as of the different orbits (with a focus on the geostationary arc) is necessary to operate satellite services on a worldwide basis.

The International Telecommunications Union (ITU), a specialized organization of the UN, is executing this management and governing the use of the radio-frequency spectrum by the international “Radio Regulations” (RR) treaty. Within the RR, it has been agreed to allocate specific frequency bands to specific SATCOM services.

The RR distinguishes the following satellite services that are used for SATCOM:

- Fixed-satellite service (FSS)
- Inter-satellite service (ISS)
- Mobile-satellite service including (MSS)
  - Land mobile-satellite service
  - Maritime mobile-satellite service
  - Aeronautical mobile-satellite service
- Broadcasting-satellite service (BSS).

With the variety of satellite frequency bands that are allocated to above satellite services and can be used for SATCOM, designations have been developed so that they can be referred to easily. Traditionally, the **C**-band (3-7GHz), **Ku**-band (10–15 GHz) and **Ka**-band (17–43 GHz) are allocated to the fixed satellite services and the **L**-band (1–2 GHz) to mobile satellite communication. All those bands are heavily exploited by commercial industry.

While there is no explicit allocation in the RR reserved for governmental or military use, agreements between governments (specifically NATO nations) exist to use the **P**-band (200–400 MHz) and the **X**-band (7–10 GHz) as well as portions of the **Ka**-band (so-called military Ka-band) for governmental (military) purposes.

The **P** (or UHF)-band is dedicated to tactical voice communications and data links, although only providing a very limited throughput. Despite being an extremely limited service in terms of throughput, UHF has become an enduring technology for troops worldwide due to its utility for highly mobile, deployed forces. This utility is unlikely to change in the future despite the availability of handheld commercial SATCOM systems such as Iridium, Thuraya, and Globalstar.

The **X**-band is considered as ideal to establish secure and robust satellite communication links, for example to connect operational areas with the homeland HQs

(reach-back), between theaters of tactical operations, maritime missions or over areas affected by a humanitarian crisis.

The military Ka-band (from 30 to 31 GHz and 43.5 to 45.5 GHz for the uplink and from 20.2 to 21.2 GHz for the downlink) provides a valuable spectrum resource in support of ISR (Intelligence Surveillance and Reconnaissance) missions. Providing high bandwidth for data-intensive applications over small terminals characterizes this band and makes it ideal for communications on the move.

The military users of governments traditionally focused on the geostationary (GEO) orbit for their SATCOM satellites. In this orbit, characterized by a flight height of almost 36,000 km above the Equator, a satellite needs exactly 1 day to fly around the earth and thus appears to be fixed above the same point on Earth. Because of this specific characteristic, a GEO orbit is very beneficial for supporting communications and earth stations are easy to install to keep the link between ground and satellite as they do not have to track the satellite's movement. This leads to lower terminal costs compared to more sophisticated terminals with the ability to track a moving satellite. Operation of terminals is also easier in GEO orbit SATCOM systems. A single satellite deployed into geostationary orbit provides visibility of almost a third of the earth's surface.

However, satellites in a geostationary orbit cannot cover the polar regions as they are invisible at latitudes higher than  $\sim 75^\circ$ . Another disadvantage of GEO SATCOM solutions is the relatively high latency they impose on communication signals due to the long distance between a GEO satellite and the Earth.

Besides the geostationary orbit, there are several *non-geostationary orbits* (NGSO) used to provide SATCOM services.

Between approximately 500 and 2000 km above the Earth, *low earth orbits* (LEOs) are implemented. Due to their little height, they can better support applications that are latency sensitive.

However, their coverage is extremely limited and their visibility above a certain point on Earth is in the range of 15 min. As one LEO satellite can only provide this visibility every 90–120 min, usually constellations of LEO satellites are used to provide uninterrupted SATCOM services. This imposes some challenges to the ground system as a signal handover from one satellite to another is necessary.

**Medium earth orbits** (MEOs) describe the region of space between LEO and GEO. They are mainly used for navigational satellites but provide also communication services. Depending on the elliptical orbit MEO satellites are in, their visibility above Earth can vary from a few hours up to half a day. To provide a global coverage, a constellation of several satellites is therefore needed.

Besides those three classical orbits, more orbits of lower relevance are used by communication satellites as some of them are very suitable to support specific use cases.

Frequency regulation constraints and orbital reservation are very significant points to be tackled early in any SATCOM project.

## **SATCOM for Military**

There is a general understanding that the provision of Satellite Communication (SATCOM) services for governmental use can be divided into three tiers which corresponds to different levels of information assurance although the exact definition of each tier may slightly vary.

### **Commercial SATCOM (COMSATCOM)**

Mass market commercial SATCOM (COMSATCOM) is operated by private companies in a competitive market. Most of the COMSATCOM market is driven by television (broadcast), but there are also much more advanced systems that involve renting or buying dedicated communication stations (hereafter referred to as “terminals”). Governmental users are a small, though a high growth market for operators of COMSATCOM, the bulk of their turnover being linked to consumer multimedia services (TV and Internet).

In terms of communication security – in particular security mechanisms to counter threats such as anti-jamming, protecting against interception and demodulation, preventing unauthorized access, detection and neutralization of unauthorized activities – the level of protection currently implemented by COMSATCOM systems is generally considered as insufficient to meet the information security requirements for military and security use cases.

In addition, COMSATCOM systems usually don't offer specific guarantees in terms of access to the resource nor the system's vulnerability to external attacks.

### **Military SATCOM (MILSATCOM)**

MILSATCOM satellites are primarily used for military missions at the national level, or in the framework of EU CSDP or NATO operations. These services are dedicated to the more critical applications requiring advanced protection (strong resistance to interference, military cryptography, resistance to nuclear events in orbit, undetectable communications, etc.).

MILSATCOM systems are technologically very similar to each other and to an extent interoperable. Security and technology are characterized as being highly specialized and largely sovereign in nature.

### **Governmental SATCOM (GOVSATCOM)**

GOVSATCOM solutions are a new SATCOM service class that fits between mass market COMSATCOM services that do not offer specific features as regards security, robustness, and availability and MILSATCOM services that usually provide

high security and guarantee levels, however, at much higher cost and thus difficult to implement for use in low- or medium-intensity crises.

GOVSATCOM means a highly available satellite communication, providing a level of security with some resilience, obtained using technological solutions available on the market with a minimum of changes.

## **Operational Needs**

Flexibility is essential in modern conflicts.

Contemporary conflicts are usually small and asymmetrical with dynamic and often difficult-to-identify enemies typically characterized as insurgent forces. Military operations have become more international and are generally led by operational headquarters geographically distant from the active operation area.

This concept is called “reach-back” and refers to the situation where resources, capabilities, and expertise are at physical distance from the area of interest, supporting the people in the area to perform their task.

The most important advantages of this concept are the safety (by using reach-back facilities, less personnel has to be present in the area of operation), the mobility (ease staff members to move while keeping informed about the situation of the operation), the flexibility (in theater, military activities are hard to predict and this concept supports resilience in operations), the improvement in logistics (less logistical effort to deploy, maintain, and remove a command post), and the detection of the forces by the enemy (having smaller and agile centers of communication, the possibility to be detected by enemies decrease).

However, immediate disadvantage is the required information support. Constraints on bandwidth need to be overcome to ensure collaboration between units as if they were physically together.

SATCOM is the only viable means to overcome this constraint, and since the early 2000s alone, the EU led more than 30 “reach-back” missions and operations all over the world with many of them still ongoing. The geographical coverage of those missions and operations has greatly varied from Africa to the North-Eastern border of Europe and from the Mediterranean Sea and the Western Balkans to Eurasia into the Middle East and Asia.

The different scenarios that have to be supported by SATCOM range from “separation of parties by force” with large size formations and requiring a reaction time within 60 days over “conflict prevention” with medium personnel effort but requiring reaction time within 30 days to “evacuation operations” involving only small numbers of personnel and foreseen reaction time within 10 days. It is worth noting that most of those scenarios can be long-term missions (over 2 years).

All that gives an indication that the different natures of those operational needs derived from above scenarios requires different SATCOM service solutions. The military is dependent on having quick and easy access to fixed and mobile satellite services supporting tactical and strategic use cases and applications spanning all over the Earth.

## Use Cases and Applications

As already addressed in the previous section, the SATCOM requirement for the “reach-back” infrastructure (strategic, operational, and tactical communication links) between tactical local networks, the deployed Force Headquarters (FHQ), and the (reach back) Operation Headquarters (OHQ) is dominant. Only with a secure and resilient SATCOM link, a command and control can be maintained functioning.

The following use cases and applications further define the military capabilities modern SATCOM systems must support:

- **ISR platforms** are increasingly utilizing high-definition optical cameras and/or high-resolution radars and other capabilities which create increasingly large amount of data that must be communicated from the remote location/platforms to locations in theater or OHQ securely, in a timely manner in order to inform operational decision making. These sensors are hosted on a range of mobile platforms, many of which are increasingly RPAS.
- **RPAS** are an increasingly deployed capability, used to extend the range of ISR and offensive capabilities by using systems which are autonomously operated or operated under human control, but which do not require human crewing. This allows them greater range and endurance. They are usually controlled and communicated by secure SATCOM links and they can carry ISR mission equipment.
- **Telemedicine** in remote and austere environments is more and more introduced in military operations. This relies on SATCOM to deliver health care services, such as access to specialists. With increasing medical capability that relies on ICT (information communication and technology), the volumes of data that need to be transmitted have risen markedly.
- **Logistics/Admin CIS** are keys to the success of modern military operations. The activities include planning for personnel deployment and cargo movements, via a complex mix of air, sea, and land routes; developing and managing cargo and asset tracking information; procurement and purchasing systems both in theater and at the rear echelons; providing in theater access to the military HR and admin systems.
- **Welfare** CIS in the digital world of military forces cannot be underestimated as their bandwidth and quality requirements will impose a challenge for SATCOM service provision. This use case embraces the provision of access to welfare services for deployed forces and supporting civilian/contract personnel. Extremely important to keep good morale, a wide range of services such as email, video conferencing, web browsing, and streaming services needs to be provided.
- **Command and Control links** commonly called C2, have to be supported in any military mission or operation. Without a safe and secure C2 link severe consequences for the conduct of any mission or operation can be expected.

## Military SATCOM Solutions and Systems

The variety and different nature of above use cases imply that they request different levels of security and guarantees of availability.

Autonomy is an additional driver in defense systems. These all have led some countries to look for their own satellite communications solutions. In order to avoid dependencies and driven by the need to possess very capable and advanced own systems, several nations have generated the development of expensive multiyear programs for national (military) SATCOM capabilities to support military- and defense-related purposes. Most of those satellites meet specific security requirements such as anti-jamming and radiation hardening and operate mainly in the classical governmental frequency bands.

However, the vast majority of military users has no access to own SATCOM resources and is either dependent on SATCOM systems of partner countries through bilateral/multilateral agreements or has to rely on commercial SATCOM service providers.

The nature of support that is requested from SATCOM ranges from the provision of only power and bandwidth to end-to end (terminal to terminal) solutions and includes anchoring and backhauling.

### United States

The United States currently owns the largest number of military SATCOM satellites, and it has developed into a nation with multiple constellations of satellites. These constellations tend to be frequency-band specific.

The United States has divided its SATCOM communications into four elements:

- Narrowband, unprotected communications using UHF – MUOS
- Wideband communications with limited protection features on X-band and Ka-band frequencies – WGS
- Protected communications with full hardening and survivability features using Ka-Band and SHF-frequencies (above 30 GHz) – AEHF
- Leased commercial satellite communications using L-band, C-band, Ku-band, and more recently X-band and UHF

**MUOS** (Mobile User Objective System) is today the most powerful UHF SATCOM constellation. It provides UHF secure voice, data, video, and network-centric communications in real time to US forces.

Most of the US military communications are supported by the **Wideband Global System** (WGS). Currently, nine satellites provide X-band and Ka-band communication services. Originally only build to support US forces and forces of allied partners Canada and Australia, the partnership over time has been extended and funding for the latest satellites has been provided also by Denmark, the Netherlands,



Luxembourg, and New Zealand in exchange for access to bandwidth from the entire global constellation.

The **AEHF** (Advanced Extremely High Frequency) SATCOM system is used to provide worldwide highly survivable and protected national communications capabilities, in support of strategic and tactical forces of the United States and its international partners.

The services provided by AEHF operate at Ka-band and SHF-band.

In summary, the WGS constellation represents the primary communications system for the U.S. Department of Defense operated alongside the specialized AEHF operated by the Air Force and the Navy's MUOS mobile communications system, while the use of UHF SATCOM solutions falls under the remit of tactical and highly mobile requirements.

## United Kingdom

The United Kingdom, as the pioneer in European governmental SATCOM, has been a military SATCOM user since the late 1960s with the Skynet 2 satellites, actually the first communication satellites to be built outside either the United States or the USSR. The United Kingdom has always opted for multisatellite constellations. Skynet 4 was the last series of UK satellites owned and operated by the UK MOD, while the Skynet 5 fleet followed a private finance initiative (PFI) program with Airbus.

The system **Skynet 5** (four satellites with each UHF- and X-band capability) provides worldwide coverage and supports the UK military forces as well as NATO forces. It is expected that UK MoD will retake ownership of the satellites fleet by 2022.

To replace the current Skynet 5 military SATCOM capability, UK awarded a noncompetitive contract with AIRBUS DS to develop and implement Skynet 6 system, integrated by space crafts, service delivery elements to manage ground operations and an enduring capability program to provide future communication system capacity beyond the next decade. The first satellite Skynet 6A is expected to be fully operational by mid-2025.

## France

France has been a member of the military SATCOM community since 1980 with Syracuse 1 and Syracuse 2 and currently operates the **Syracuse 3** constellation (2 satellites). The Syracuse 3 series is hardened and protected to meet NATO standards, similarly to the UK Skynet series, and concentrating on military X-band frequencies to support the French military. It is significant to note that France developed the highly resilient M21 modem, compliant with NATO STANAGS, as one of the key elements of the ground segment under Syracuse 3 program, which complements and supports tactical SATCOM networks.

With a look into future capabilities in SATCOM, in December 2015, France ordered the first two **Syracuse 4** satellites from Thales-Alenia Space and AIRBUS as the main elements of the future program COMSAT-NG. The new satellites, with specifications to be threat resistant to cyber-attacks, jamming, and HANE events, are expected to meet full operational capability from 2022.

The French position with regard to multinational SATCOM capabilities development is based on a vision of different layers that contribute to the overall SATCOM capability. The **SICRAL 2**, a joint Italian-French military SATCOM program, operates in X-band and augments the Syracuse system. This can be considered as core capacity for military use only. On the other side, as an extension of core capacity for use of military and government users, the **Athena-Fidus**, a French-Italian joint-venture, is a geosynchronous military and governmental Ka-band communications satellite capable of data transfer rates of up to 3 Gbps. Jointly procured by the French and Italian space agencies and defense procurement agencies, the system is intended to be used by the French and Italian armed forces as well as the civil protection services of France and Italy.

Besides those own resources, France has long-term contracts in place for leasing commercial SATCOM capacity that complements the national systems.

## Germany

Germany has only recently entered the military SATCOM arena with its own dedicated assets after relying for many years on NATO capacity, intergovernmental agreements, and commercial leases.

The German Bundeswehr has launched **COMSATBw 1** and **2** in October 2009 and June 2010, respectively, as part of its SatComBw-Stage 2 program and operates the two satellites with industrial support. Both satellites are identical carrying UHF- and X-band payloads. Besides those own resources, Germany has long-term contracts in place for leasing commercial SATCOM capacity.

Germany is currently defining requirements for the future systems replacing the existing SATCOMBw-Stage 2 capacities. COMSAT 1 and 2 satellites will reach their end of life by 2027. With this regard, the options include different models for acquisition of SATCOM capacity, from lease to cooperation with third party programs, also including future EU and NATO programs.

In addition, a recent contract has been signed between Germany's Deutsche Zentrum für Luft- und Raumfahrt (DLR) (on behalf of the German MoD) with OHB systems to develop a dual-use satellite using the SmallGEO platform, Heinrich Hertz, operating in Ku and military Ka bands. The satellite is expected to be fully operational by 2021.

## Italy

Italy, with **SICRAL 1A**, launched the first military satellite communication spacecraft in 2001 into geostationary orbit, providing UHF and X-band capacity to Italian armed

forces and also (jointly with France and the United Kingdom) to NATO forces. The second phase of the program began in 2009 with the launch of SICAL 1B.

The third phase of SICRAL program, the **SICRAL 2**, a joint Italian-French military SATCOM program, became operational in 2015. SICRAL 2 is a geostationary satellite that operates in X- and UHF bands, supports satellite communications requirements of Italian and French Armed Forces, and is able to enhance the SATCOM capabilities and provide backup to the Italian SICRAL 1 and French Syracuse 3 systems.

Italy is planning resources' allocation to maintain the capability of the SICRAL satellites, and further resources may be added by the National Space Programme for the acquisition of the SICRAL 3 system for strategic communications replacing or complementing the current systems.

## Spain

Since 2005, Hisdesat (a company shared by the Spanish MoD and Spanish industrial players) is providing secure satellite communications services to the Spanish Ministry of Defence. With **SpainSat** and **Xtar-EUR**, Hisdesat has an innovative generation of satellites that provide satellite communication services in the X and military Ka bands.

Spain is currently working to replace the XTAR-EUR and Spainsat satellites that will reach the end of their final operational capability (after propellant savings) between 2022 and 2024. In this regard, the future satellite communications program, **SPAINSAT-NG**, has been approved in April 2019 and will encompass a space segment consisting of two highly protected threat-resistant satellites operating X-, military Ka-, and UHF bands, improved ground segment deploying new satellite terminals implementing EPM anti-jamming capabilities, and an additional enhanced anchor station. The SPAINSAT-NG will meet the operational capability by 2024.

## Luxemburg

The youngest member of the European SATCOM-owning states launched its first satellite in early 2018. **GovSat-1** is a GEO multimission communication satellite operated by LuxGovSat, a public-private joint venture created in 2015 between the Government of Luxemburg and commercial satellite operator SES.

GovSat-1 was built by Orbital ATK and is offering 68 transponder-equivalent units of 36 MHz. Positioned at 21.5° East, it will provide satellite communications services within Europe, the Middle East and Africa, and enable operations over the Mediterranean, Atlantic, and Indian waters.

GovSat-1 was designed for dual-use to support both defense and civil security applications, including mobile and fixed communications. The satellite provides X-band and military Ka-band services on high-power and fully steerable mission beams. Equipped with anti-jamming features, encrypted telemetry, and control,

GovSat-1 will provide enhanced resilience capabilities to meet requirements of governmental and military users and targeting to support the future demands of NATO members.

Luxembourg has currently launched the initial phases to develop an additional GovSat-2 satellite to further enhance the available SATCOM capacities and services.

## Other European Activities

Most European nations, other than the ones mentioned above, have neither the budget nor the depth and breadth of requirements to justify investment in own dedicated satellite capability. These nations have typically used intergovernmental agreements with their allies to gain access to protected communications (Germany did this with France for many years prior to launching the SatComBw programs).

When intergovernmental agreements are not possible, then long- or short-term lease contracts with commercial operators or service providers have often proved to be the vehicle of choice.

Nearly every nation has now leased one or more services from Inmarsat to include within its military portfolio for maritime or airborne communications, and this has been augmented over the last 5–10 years with leases of Intelsat, SES, or Eutelsat capacity and more recently with commercial X-band communications leased from either Paradigm or XTAR systems. These nations include, among others, Belgium, Czech Republic, Denmark, the Netherlands, Poland, Portugal, or Slovenia.

The launch of the Inmarsat GLOBAL Xpress but also other new satellite systems like high-throughput satellites will likely increase this usage.

In addition to above bilateral or commercial SATCOM service solutions, the 26 participating Member States of the European Defence Agency can meet their SATCOM requirements through two specific projects established in the Agency:

- **EDA GOVSATCOM Pooling and Sharing Demonstration Project (GSC Demo):** The main goal of this project is to prove and demonstrate the concept and benefits of a collaborative Pooling and Sharing model in GOVSATCOM and meet the **GOVSATCOM** demand of Member States and European CSDP actors through a pooled capability (bandwidth/power and/or services) provided by contributing Member States. By pooling the capability of the Member States, the project provides Governmental SATCOM services to the members, contributing to the overall operational efficiency. The project aims to demonstrate an efficient pay-per-use solution that does not impose any binding financial commitments beyond services requested. It is quick and flexible, establishing government-to-government agreements through EDA and so reducing the administrative burden for members who do not have to run their own GOVSATCOM capability. There are currently 15 contributing members to the GSC Demo project.
- **EDA – European Union Satellite Communication Market (EU SATCOM Market):** Mainly addressing COMSATCOM solutions, the EU SATCOM

Market (formerly known as European Satellite Communications Procurement Cell (ESCPC)) was launched in 2009. The project's aim to provide **commercially** available satellite communications (fixed and mobile) as well as related services (e.g., feasibility studies, maintenance, leasing of earth stations, SATCOM terminals, commercial crypto solutions) and options for other communication services for operations (e.g., theater local radio network, IT network backbone for the field headquarters) through the establishment of a number of Framework Agreements on behalf of the contributing members, to promote ease of access and improve efficiency. This project is now fully operational with a growing number of members and orders intake for long duration. The current contract will expire in January 2020 and will be renewed. There are currently 28 contributing members to the EU SATCOM Market including almost all CSDP military and civilian operations and missions.

## **NATO**

For almost 20 years, NATO owned and operated the two NATO IVA and IVB satellites by itself. In May 2004, the NATO Consultation, Command and Control Agency (NC3A) decided to move away from owning and operating its own fleet of satellites and selected a multinational proposal to provide SHF and UHF communications. This program, entitled the NATO SATCOM Post-2000 (**NSP2K**) program, was based on the support of the French, Italian, and British governments to provide NATO with access to the military segment of their national satellite communications systems – Syracuse, SICRAL, and Skynet, respectively – under a Memorandum of Understanding (MoU). Compared to the previous NATO-owned capabilities, this policy change resulted in increased bandwidth, coverage, and expanded capacity for voice and data communications, including communications with ships at sea, air assets, and troops deployed across the globe.

Currently, the successor program is under discussion, under NATO Capability Package (CP9A0130) “Satellite Communications (SATCOM) Transmission Services.” Through this CP130, the acquisition (common-funded) roadmap will address the renewal of allied SATCOM capacity for the period 2020–2034 across areas corresponding to the military SATCOM frequency bands (i.e., X-band, or SHF, EHF, UHF, and Military Ka-band).

## **Russia**

Russia (former USSR) was the first country to orbit a satellite in 1957. It is reported that between 1960 and 1990, most Soviet satellites that were launched carried military payloads, even though until the last decade of the twentieth century there was no official acknowledgment of a military space program. During the first decade of the twenty-first century, Russia has continued its launch program and now identifies specific military satellites but with no specific information as to individual missions.

---

## China

China launched its first satellite in 1970. Since then, its satellite activity has increased, particularly in the last decade of the twentieth century and the first decade of the twenty-first century. China has a large program of both reconnaissance and communications satellites utilized for military purposes.

China utilizes communications satellites for both regional and international telecommunications supporting both military and commercial users somewhat like several other countries.

---

## SATCOM for Security

### European Union (EU)

In December 2013, the Heads of States and Government of the EU met to discuss defense and the Common Security and Defence Policy. In the Conclusions, the European Council *“welcomed the Commission communication ‘Towards a more competitive and efficient defence and security sector.’ More specifically, the European Council welcomed plans regarding SATCOM: ‘preparations for the next generation of Governmental Satellite Communication through close cooperation between the Member States, the Commission and the European Space Agency; a users’ group should be set up in 2014; the European Council invites the Council, the Commission, the High Representative, the European Defence Agency and the Member States, within their respective spheres of competence, to take determined and verifiable steps to implement the orientations set out above.’”*

That was a response to the growing needs identified in terms of secured and guaranteed access for institutional users and the starting point for several activities on European level to improve security and achieve guaranteed access to SATCOM for EU Member States and actors.

The Global Strategy for the EU Foreign and Security Policy (EUGS) issued in June 2016 stresses the importance of capabilities that should be developed with maximum interoperability and commonality and puts forward the objective of promoting the autonomy and security of European space-based services. *“European security hinges on better and shared assessments of internal and external threats and challenges. Europeans must improve the monitoring and control of flows which have security implications. This requires investing in Intelligence, Surveillance and Reconnaissance, including [. . .] satellite communications, and autonomous access to space and permanent earth observation.”* The EUGS claims that *“Defence policy also needs to be better linked to policies covering the internal market, industry and space.”*

The High Representative for Foreign Affairs and Security Policy (HRVP), through the EUGS, has thus emphasized that *“Member States need all major equipment to respond to external crises and keep Europe safe. This means having full-spectrum land, air, space, and maritime capabilities.”*

Building on the Global Strategy and in the frame of protection of the EU and its citizens, the Implementation Plan for the EUGS, issued in November 2016, states the EU can contribute to ensuring stable access to and use of the global commons, including the high seas and space. Taking forward the cross-cutting strategies in the domain of space (including in relation to the Copernicus and Galileo programs) and their links to CSDP, evolutions in the security and defense environment require the EU to reassess its space capabilities in areas relevant to Europe in the context of specific security needs. The Implementation Plan further stresses the needs to invest and develop collaborative approaches in satellite communications, autonomous access to space, positioning navigation and timing (PNT), and permanent earth observation.

The Space Strategy for Europe (SSE), issued by the European Commission in October 2016, describes space as a strategic asset for Europe. The SSE reinforces Europe's role as a stronger global player and is an asset for its security and defense. To increase security, satellite PNT, satellite communications, and Space-Based Earth Observation have been identified as crucial to contribute *inter alia* to detecting illegal immigration, preventing cross-border organized crime, and combating piracy at sea. The SSE describes emerging needs related to security and defense. "Space capacities are strategically important to civil-, commercial-, security-, and defense-related policy objectives. Europe needs to ensure its freedom of action and autonomy. It needs to have access to space and be able to use it safely. Due to growing threats emerging in space (from space debris to cyber threats), greater synergies between civil and defense aspects" will become "increasingly relevant" to reduce cost, increase resilience, and improve efficiency. Europe must draw on its assets and use space capacities to meet the security and safety needs of the Member States and the EU.

The draft EU Legislative Proposal for the EU Space Programme for the next multiannual financial framework (MFF 2021–2027), issued in June 2018, reflects the increased relevance of security and defense, synergies between civil and defense technologies, and applications of space-based assets and services and the potential applications resulting from the EU Space Programme components. EU GOVSATCOM, a new activity proposed by the European Commission, is one of the four Programme Components foreseen within the EU Space Programme. The European Commission intends to establish a Pooling and Sharing solution based on already available and foreseen commercial and governmental SATCOM resources.

## **European Space Agency (ESA)**

The European Space Agency (ESA) has recognized that "the demand for secure satellite communications is increasing worldwide. Satellite communications have become part of the Digital Economy and are increasingly integrated into terrestrial solutions. In order to remain a reliable element in times of increasing cyber-threats, the satellite component needs to evolve and provide the resilience and cybersecurity expected in a commercial market. Furthermore, reliable and secured

communications are more and more required in an institutional governmental setting. They support increasing societal needs such as for crisis management, maritime safety, and border control, which are also reflected in Europe's proposal for EU GOVSATCOM."

Therefore, and to underline ESA's contribution to the European goal to "ensure European autonomy in accessing and using space in a safe and secure environment," ESA is investing huge efforts in a variety of actions on Secure SATCOM for Safety & Security (4S), with the ESA GOVSATCOM Precursor activities as specific element responding to the growing need in Europe for secure communications for applications such as crisis management and maritime safety.

---

## **Conclusion, Outlook and Perspectives**

SATCOM for defense and security will remain to represent of crucial support for a plethora of military and security applications.

The current activities, in particular at EU level, to achieve a GOVSATCOM capability for military and civilian security users describe already how the future of SATCOM for defense and security will look like.

Those users will more and more rely on solutions that are provided from both governmental and commercial resources. However, the commercial SATCOM service providers will have to proof that they will be able to meet the security requirements defined by the defense and security users and that they are also able to provide a resilient service whenever a need arises. Commercial SATCOM service providers have realized the challenge to improve the security within their satellite systems and activities are ongoing in this direction.

Satellite capacity should not be a scarce resource with the upcoming new commercial activities on (V)HTS. New applications like near-real-time video-on-demand and high-speed internet can create new use cases. In addition, the use of those commercial resources should be still affordable for defense and security users.

From a technical point of view, defense and security users will also benefit from ongoing innovations and implementations of advanced solutions for SATCOM systems.

GEO satellites will remain the main source of all SATCOM provisions. However, with the upcoming LEO and MEO constellations, new technical solutions will be offered and new use cases, which so far could not be supported by SATCOM due to specific latency requirements, are thinkable. The constellation approach is also promising in respect of cost reductions as standardization will lead to lower capital expenditures.

Further innovations that will contribute to military capabilities directly or indirectly are the use of electric propulsion that will allow to significantly reduce the satellite mass at launch allowing heavier payload and therefore more efficient satellites, having additional effects on cost and affordability and laser communications that will significantly increase security and data rates in SATCOM systems.



The commercial market and the defense and security users will therefore come even closer and classical high-security SATCOM solutions will become more and more the exemption, focused on very specific use cases and remain to be in the stock of only a few countries that again could make available those resources to partners.

---

## References

- A Global Strategy (GS) for the European Union's Foreign and Security Policy (2016) EEAS
- EUROPEAN COUNCIL (2013) EUCO 217/13, EUROPEAN COUNCIL 19/20 DECEMBER 2013, CONCLUSIONS
- EUROPEAN EXTERNAL ACTION SERVICE (2016) Shared Vision, Common Action: A Stronger Europe - A Global Strategy for the European Union's Foreign and Security Policy
- EUROPEAN COMMISSION (2016) COM (2016) 705 final, Space Strategy for Europe
- EUROPEAN DEFENCE AGENCY (2017) Governmental Satellite Communication (GOVSATCOM) - Feasibility Study, EUROCONSULT
- EUROPEAN SPACE AGENCY, <https://artes.esa.int/4s-govsatcom-precursor>
- Fritz DA et al. (2006) Military Satellite Communications: Space-Based Communications for the Global Information Grid, Johns Hopkins APL Technical Digest, 27(1)
- Governmental Satellite Communication (GOVSATCOM) feasibility study (2017) EUROCONSULT
- NATO (2014) Reference Catalogue of the Existing and Planned UHF, SHF and EHF Satellite Communications Equipment, NATO
- Reference Catalogue of the Existing and Planned UHF, SHF and EHF Satellite Communications Equipment (2014) NATO
- Space Strategy for Europe (SSE) (2016) European Commission



# Position, Navigation, and Timing for Security

# 42

Jean-Christophe Martin

## Contents

Introduction .....	798
Overview of Existing GNSS .....	799
Description and Development of GNSS Systems .....	800
Concept of GNSS Interoperability .....	809
Vulnerabilities of GNSS Services .....	811
Deliberate Threats to GNSS Services .....	812
GNSS Applications Relevant for Security .....	814
PMR: A Combined Use of GNSS and TETRA/TETRAPOL (Fig. 11) .....	814
GNSS, Galileo, and Timing for Secured Applications .....	816
The PRS and the Brexit .....	817
Conclusions .....	818
References .....	818

## Abstract

Global Navigation Satellite Systems (GNSS) allow users to compute their position, velocity, and time anywhere in the world, anytime, and with a high accuracy. The best known and most popular GNSS is the US Global Positioning System (GPS), far in front of the Russian GLONASS system. However, due to the strategic importance of the GNSS, other powerful nations are developing their own global systems (GNSS): the European Union's (EU) Galileo and China's BeiDou, also known as KOMPASS.

**Galileo may reach the FOC (full operational constellation) with 30 satellites (24 operational and 6 spare) in middle orbit in 2020/2021.** BeiDou, the Chinese constellation, may also reach its FOC with five geosynchronous and

---

J.-C. Martin (✉)

CEO Marency SAS, Paris, France

CEO Marency SAS, Brussels, Belgium

e-mail: [jcm@marency.eu](mailto:jcm@marency.eu); [jcm.marencyconsulting@gmail.com](mailto:jcm.marencyconsulting@gmail.com)

27 satellites in middle orbit at the same moment. It means that each citizen on the Earth may be able to use the four constellations (GPS, Galileo, BeiDou, GLONASS), given that they have the proper receiver and chip. The combined capacity of the four constellations makes around 120 satellites around the Earth, and at least 15 satellites in view of each user begin in 2021. This makes a tremendous benefit and creates a multitude of opportunities for many applications and in particular for some secured applications, such as certain secured IoT (Internet of Things) or timing applications.

GNSS mainly offers two types of services: an open service, available to anyone, and an authorized service, providing better performance and available only to authorized users. The authorized services already support the defense military operations of the USA and Russia, while the open services have become instrumental for security in general and for civil security operations of any state supporting, for instance, police and civil protection. The fact that there is an opened service (OS) does not mean that secured applications cannot be developed relying on open services. The fact that a user can develop applications relying on four constellations (GPS, Galileo, BeiDou, and GLONASS) gives a huge number of applications for authentication, for example (applications on which the user is sure that he is using the right signals).

Galileo (and also the three other constellations) offers a specific service k called “Public Regulated Service” (PRS). Its “spectrum of applications” is broader than defense only but is “security” in a larger way. Each member state of the European Union, with the proper security organization, can use the PRS for its secured applications (police, special services, civil security, customs, etc.). This chapter addresses in particular these aspects, the use of the Global Navigation Satellite Systems (GNSS) for security applications.

---

## Introduction

GNSS is the generic term for space-based systems that transmit signals that can be used to provide three services: position, navigation, and timing (PNT). The best known and most popular of the GNSS is the US Global Positioning System (GPS), although the Russian GLONASS system is regaining strength and other systems are being developed, such as EU’s Galileo and China’s BeiDou.

Some regional systems are also developed: IRNSS (Indian Regional Navigation Satellite System) by India and QZSS (Quasi-Zenith Satellite System) by Japan; the USA have their own SBAS system, WAAS (Wide Area Augmentation System), and Europe has developed EGNOS (European Geostationary Navigation Overlay Service). EGNOS is a geostationary system which, by improving the GPS signals over Europe, addresses very stringent users such as aeronautic or maritime users, for instance, or rail users, and surprisingly, agriculture, as they have very tough economic constraints. Some users have got precision constraints (the need to optimize the manure spreading of fertilizer in agriculture) or high constraints on integrity (rail), which is the parameter characterizing the trust the user can have in the signal

(the signal reception is not always perfect, and the receiver often uses an algorithm called RAIM – receiver autonomous integrity monitoring – which assess the quality of the signal).

PNT applications are a domain in constant expansion with about 120 GNSS operational satellites (available in 2021), compared to the 30 satellites of GPS used by most applications in the year 2010. The development of IoT – Internet of Things– and connected device may rely for a part on GNSS concepts and PNT for logistics and scientific applications, for example. The consumption of the device, the receiver, is a major difficulty for the permanent use of GNSS, but IoT worldwide can use GNSS signals part time, for example, to improve the duration of the battery. As soon as you combine PNT device, a device which accesses to its PNT, and a telecommunication function, you open a huge number of applications, in particular secured ones.

The security applications for these technologies are extremely large. A wide security and civilian community can benefit from space services such as GNSS in support of strategic economic and commercial activities, strategic and critical transport, internal security (e.g., civil protection, firemen), law enforcement (police, professional mobile radio using TETRA or TETRAPOL standards), emergency services, customs, critical telecommunications, and critical energy.

---

## Overview of Existing GNSS

Global Navigation Satellite Systems (GNSS) are experiencing a new era. The US Global Positioning System (GPS) now serves over a billion of users in a bewildering breadth of applications. The Russian system GLONASS is helpful but has never reached such figures (the order of magnitude of GLONASS users is of a few millions worldwide, mainly through chips in smartphones) but is increasing thanks to the mobile phones and their chips using all the available GNSS. China has invested and has developed its system known as BeiDou or Compass, with a constellation of 27 MEO satellites, 3 geosynchronous satellites, and 5 geostationary Earth orbit (GEO) with a global constellation which may be operational around 2021.

In addition, the European Union is developing the Galileo system, a GNSS that promises to place 24 satellites in medium Earth orbit (MEO) plus 6 spares in 2021. In 2019, 26 Galileo GEO satellites are in orbit and 24 GEO are operational (due to the fact that two satellites, which are active, were injected on a bad orbit in 2014 by a Proton/Soyuz launcher). “Initial services” became available on 15 December 2016. Then as the constellation is built-up beyond that, new services will be tested and made available, with system completion scheduled for 2020/2021. Once this is achieved, the Galileo navigation signals will provide good coverage even at latitudes up to 75 degrees north, which corresponds to Norway’s North Cape – the most northerly tip of Europe – and beyond. The large number of satellites together with the carefully optimized constellation design, plus the availability of the three active spare satellites per orbital plane, will ensure that the loss of one satellite should have no discernible effect on the user.

Furthermore, in Europe, EGNOS (European Geostationary Navigation Overlay Service) is made of three geostationary satellites and a ground segment, which augments the existing GPS constellation by providing integrity and improved accuracy. EGNOS has been operational for aviation for more than 5 years. The USA has a similar operational augmentation system called WAAS (Wide Area Augmentation System). Furthermore, India and Japan are developing their own regional systems, respectively, IRNSS (Indian Regional Navigation Satellite System) and QZSS (Quasi-Zenith Satellite System), which will provide positioning and augmentation services (Fig. 1).

## Description and Development of GNSS Systems

Detailed description of all GNSS has been published by the United Nations International Committee on GNSS (UN ICG). The UN ICG is an informal body of the UNOOSA (United Nations Office for Outer Space Affairs) with the purpose of promoting cooperation on civil satellite-based positioning, navigation, timing, and value-added services, as well as compatibility and interoperability among the GNSS systems, while increasing their use to support sustainable development, particularly in the developing countries. The participants are the GNSS providers (e.g., the USA for GPS and the European Union for Galileo) as well as various user communities. They have published different interesting documents to support space and GNSS (or Earth observation) in 2018, such as “European Global Navigation Satellite System and Copernicus: Supporting the Sustainable Development Goals. Building Blocks towards the 2030 Agenda” or “The Interoperable Global Navigation Satellite Systems Space Service Volume” in October 2018.



**Fig. 1** Artist view of the ejection of the two first Galileo satellites with a Soyuz launcher

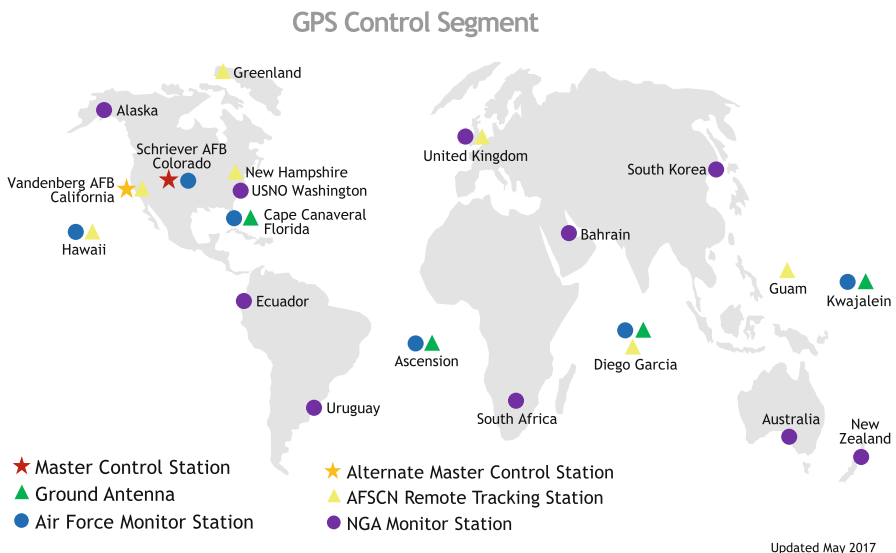
### The US Global Positioning System

The GPS has been designed by the Department of Defense (DoD) in the 1970s to meet military requirements: at the beginning, it has been used to improve the navigation of the US ballistic missiles. The Navy, Air Force, and Army each came up with their own designs and ideas, and in 1973, a design was approved by the US government. It was also in parallel quickly adopted by the civilian world. The first satellite for the NAVSTAR GPS was launched in 1974, and from 1978 to 1985, another 11 were launched for testing purposes. The full nominal constellation of 24, which today allows navigation system to use worldwide GPS coverage, was completed in 1993. Currently, the GPS satellite constellation includes more than 30 operational satellites.

To understand the concept, the system comprises also the ground segment, with the ground control and its stations worldwide, which is key for the performance of the system, its security, and its availability (Fig. 2) (Kaplan and Hegarty 2017).

As said, initially, GPS was only intended for military use, even for very strategic applications linked to the performances of their ICBM (intercontinental ballistic missiles). **On 1 September 1983**, Korean Airlines flight KAL 007 from Anchorage to Seoul strayed off course into USSR airspace and was shot down by a soviet Su-15 fighter jet. All 269 passengers and crew were killed. Two weeks later, **US President Reagan suggested to use GPS for civilian purpose** to avoid further dangerous navigational mistakes.

The US government included a function called selective availability (SA) into NAVSTAR GPS that would degrade its accuracy (by a factor of 10) for civilian users to ensure no enemy or terrorist group could use GPS to make accurate weapons. It



**Fig. 2** Ground segment of the GPS system

has worked introducing deliberate errors into the data broadcast by each satellite. Military users could access the fully accurate system by using an encrypted signal that was broadcasted simultaneously but not available to unauthorized users. During the Gulf War, GPS became a strategic technology for the US military, which needed many more GPS receivers than it had. It is solved by using civilian GPS receivers; but to increase the accuracy of these devices, the SA function had to be temporarily disabled. Then, in 2000, US President Clinton announced that SA would be disabled completely, as US government “threat assessments” concluded that removing SA would have minimal impact on national security. He also said that the USA would still be able to “selectively deny” GPS signals on a regional basis; it means the local jamming of a zone. This concept is known as “NAVWAR” in the military world.

In the civil world, this concept could be used – even if it has not been used yet – for security reasons, in case of a “hard riot,” for example, in a town, to allow only security forces to use GNSS as authorized users. It is particularly interesting as this concept can give an operational superiority to police toward “hard rioting demonstrators” who are very mobile while using social networks.

GPS provides two types of services: a standard positioning service (SPS) and a precise positioning service (PPS). Authorized access to the PPS is restricted to the US Armed Forces (USAF), federal agencies, and selected allied armed forces and governments. The SPS is available to all users worldwide on a continuous basis and without any direct user charge. The specific capabilities provided by the GPS open service are totally opened. They are published in the GPS Standard Positioning Service Performance Standards ([www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf](http://www.gps.gov/technical/ps/2008-SPS-performance-standard.pdf)).

Likewise GPS, most space-based PNT systems will provide two types of services: an open service (OS) and an authorized service (AS). The UN ICG (see section “Description and Development of GNSS Systems”) has proposed the following definitions:

- **Authorized Service:** a service which is specifically designed to meet the needs of authorized users in support of governmental functions (e.g., the PPS (P(Y) and the M-Code) for the military GPS and the PRS – Public Regulated Service – for Galileo authorized users by the governments); these services are encrypted with a high level of encryption, to be used by “authorized only” users; these types of signals are also deployed on the GLONASS and on the BeiDou system.
- **Open Service:** service (using one or more signals) provided to users free of direct user charges; the four GNSS have got such a service, available for all users; their detailed definition is free, opened, and published worldwide for the signal, in a specific document, called an ICD – (interface control document).

In addition to these two services, other types of GNSS services exist, such as the Galileo commercial service, which will provide added-value data to users who may have to pay for it. It will provide, for example, the capability of authentication of the signal which could be of interest for secured and legal applications. It means, for example, that users who need to be able to proof their position or timing on some

applications, toward a tribunal, for instance, could use this encrypted commercial signal. Other applications even secured are foreseen for applications with needs which are commercially important but not as secured as for PRS applications.

### GPS Modernization (Fig. 3)

The GPS modernization program upgrades the GPS space and control segments with new features to improve GPS performance, which include new civilian and military signals. GPS modernization is in particular introducing modern technologies throughout the space and control segments that enhance overall performance. The military are using the PPS (Precise Positioning Service), which is an encrypted signal that can only be used by military or users authorized by military such as coast guards. The USA has developed a new PPS signal, named M Code, which is also encrypted and dedicated to military users. The constellation (30 satellites) and the receivers are changed. But the user are “military only” (even if there are some exceptions such as the coast guards in the USA). Whereas for Galileo, the use of the PRS, which is foreseen and under the total control of the member states (who decide



**Fig. 3** A GPS III-A, the last generation of GPS satellites



who their users are), is totally “security oriented” but broader than the PPS in terms of applications and users.

It should be pointed out that technical and political exchanges have permitted to define jointly the next generation of open signals, the GPS III SPS and the Galileo OS (Hein et al. 2001). Thanks to “the Signal Task Force,” created in 2000 by the European Commission and the member states, ESA, and the Commission, following 4 years of technical exchanges with the USA, that have defined Galileo’s signals (Status of Galileo Frequency and Signal Design 2002). GPS III’s SPS signal and Galileo OS are therefore fully compatible, thanks to this excellent cooperation between the USA and the European teams.

The USA also developed a so-called satellite-based augmentation system (SBAS) named WAAS (Wide Area Augmentation System) over the US territory, relying on geostationary satellites, the system that improves the performance of the GPS constellation. The geo-satellites provide corrections to the user and to the signal propagation errors in the atmosphere and integrity monitoring. It is extremely useful for civil aviation over the US territory, principally for precision approach procedures down to 200 feet.

### **The Russian GLONASS System**

Flight tests of high-altitude satellite navigation system, called GLONASS, started in October 1982 with the launch of the Kosmos-1413. The GLONASS system was brought into operational testing in 1993, and the whole orbit group of 24 satellites was formed in 1995. However, decrease in funding for space industry in 1990 led to the degradation of the GLONASS constellation. Russia has increased its contribution to the GLONASS constellation and could have spent around 10Md€ on its satellite navigation system on the period 2012–2020.

For the last 20 years, one of the major differences between GLONASS and both GPS and Galileo has been the choice of the management of the frequency bands and signals. The concept of sharing out frequencies is different for GLONASS than for GPS or Galileo. GLONASS uses one frequency for each pair of satellites (around the Earth at opposite sides). This leads to the use of 15 different frequencies for the constellation, the 30 satellites (so-called FDMA (Frequency division multiple access) techniques). There has been discussion between the European Commission and Russia in the year 2000: Russia wanted Galileo to use the FDMA concept. However, Galileo chose the CDMA (Code division multiple access: a multiplexing scheme is used to allow all the satellites of the constellation to use the same frequency. In fact, it is a bit more complicated as GPS and Galileo are using three different ranges of signals for different types of applications (see References 1 and 2 on E1/L1, E5, and E6 bands.) techniques, like GPS. Therefore, for the open service, GPS and Galileo are using one frequency for all their 60 satellites (Galileo uses three different frequencies and bands, like GPS, but two only are the same). This difference between the two modulations (CDMA versus FDMA) implies an interoperability complexity; combined GPS/GLONASS receivers were until recently more expensive and more complex. Thanks to improvements in semiconductor technologies over the past years, receiver manufacturers have managed to produce chips and receivers able to receive the four

constellations – GPS, Galileo, GLONASS, and BeiDou – at a very reasonable cost and complexity level. It is in particular the case for smartphones such as iPhone or Samsung. Furthermore, GLONASS has conducted a modernization process, which has improved its interoperability with the other GNSS, through the choice of CDMA management of signals and frequencies. The interface control documents for GLONASS CDMA signals have been published in August 2016.

The first generation of GLONASS satellite was designed with a 3 years' lifetime, while the real operational life was of 4.5 years. In total, 81 satellites were launched. The second generation, known as GLONASS-M, was designed for 7 years' lifetime. The last recent generations of satellites, GLONASS-K1 and GLONASS-K2, are designed for a 10 years' lifetime.

Enhanced GLONASS-K1 and GLONASS-K2 satellites, to be launched in 2019 and after, may feature a full suite of modernized CDMA signals in the existing L1 and L2 bands, which include L1SC, L1OC, L2SC, and L2OC, as well as the L3OC signal. GLONASS-K series should gradually replace existing satellites. GLONASS-KM satellites may be launched by 2025. Additional open signals are being studied for these satellites, based on frequencies and formats used by existing GPS, Galileo, and BeiDou/Compass signals:

- Open signal L1OCM centered at 1575.42 MHz, close to GPS L1C and Galileo signal E1.
- Open signal L5OCM centered at 1176.45 MHz, close to the GPS L5 and Galileo signal E5A.
- Open signal L3OCM centered at 1207.14 MHz, close to Galileo signal E5B.

Users can access the GLONASS open signals. For classical applications, such as PDA devices, the use of the four constellations can be foreseen. It means that for some secured applications for worldwide users, the use of the four constellations (GPS, Galileo, BeiDou, and GLONASS) can be expected. Concerning trusted secured applications, the use of two constellations, GPS and Galileo, is easier to manage, in four bands of frequencies (E1/L1, E5/L5, E6, L2) which are complementary and have different constraints (e.g., L2 and E6 offer different solutions for compatibility with radar bands) (Fig. 4).

### **The Chinese BeiDou (Compass) System**

In the year 2000, China has expressed its will to become a full partner of the Galileo program. They have offered 1 Md€ to become full member and in particular to access the Galileo PRS. The member states were not in favor of this option, leading to a strong willingness of China to develop its own program. The first studies have been launched around 2003. They have put a lot of pressure on their industry and have demonstrated their capability to be able to deploy a FOC (full operational capability) – around 2020/2021. On 14 April 2007, the first MEO satellite, named Compass-M1, was launched. On 15 April 2009, the first geostationary satellite, named Compass-G2, was launched. The Compass/BeiDou Navigation Satellite System was, as a first step, covering China and the nearby area in 2015. As of



**Fig. 4** Artist view: last GLONASS-M satellite

December 2018, 15 BeiDou-3 satellites have been launched. This comprises five GEO satellites, 27 MEOs, and 3 in inclined geostationary orbit (IGSO). The launch occurs from spatial center XSLC of Xichang with a launcher CZ-3B, which puts in orbit two BeiDou-3 satellites each time for a total mass of around 2 tons. Designed by CALT (China Academy of Launch Vehicle Technology), a subsidiary of Aerospace Chinese group CASC, the CZ-3B belongs to the CZ-3A family launchers, which are usually used to put in orbit geostationary satellites. The current plan is to achieve a fully operational constellation (FOC) of 35 satellites by 2020/2021.

The Compass/BeiDou Navigation Satellite System in terms of functionality is very similar to the GPS or Galileo. BeiDou is able to provide two types of service worldwide: an open service and an authorized service. The open service provides, like GPS or Galileo, free positioning, velocity, and timing service. The authorized service should provide encrypted positioning, velocity, and timing services for authorized users (military users) (Fig. 5).

### **The European GNSS Galileo and EGNOS Systems**

The Galileo program is Europe's initiative for a state-of-the-art global satellite navigation system, providing a highly accurate, guaranteed global positioning service worldwide. The program started in the European Commission, in 1998, with the so-called GNSS2 initiative. The system consists of 30 satellites, 24 operational and 6 spare, and the associated ground infrastructure. Galileo is interoperable with the GPS system (the signals have been commonly defined). Unlike GPS, Galileo is not a military system. It means that the system is not designed as a military system, with some nuclear resilience, for example. A Galileo satellite weight is about 600 kg versus 2 tons for a GPS satellite. However, Galileo can be used for security and



**Fig. 5** Launch of BeiDou satellites

defense applications because each member state of the European Union is sovereign in choosing its users. When Galileo was designed, two main technical risks were identified: the “spatialization” of the atomic clocks and the management of the constellation (30 satellites). Even if there has been some technical difficulties on Galileo satellites, with the first generation of onboard European atomic clocks, this was probably the “price to pay” to develop an autonomous capability on such a critical technology in Europe. These technical risks have now been well identified and managed.

Galileo provides the European Union with an autonomous access to satellite navigation, a technology used in sectors that have become very important for its economy (about 7% of the EU GDD) and the well-being of its citizens. The market for satellite navigation services has been growing steadily and is expected to be worth €250 billion per year by 2022. Whereas EGNOS is operational since 2011, Galileo will become fully operational worldwide as GNSS in 2021 (FOC – full operational capability) (Fig. 6).

Independent studies show that Galileo may deliver around 90 billion euros to the EU economy over the first 20 years of operations, in the form of direct revenues for the space, receivers, and application industries and in the form of indirect revenues for society (more effective transport systems, more effective rescue operations, etc.).

A huge range of innovative applications is foreseen, such as improving air traffic management and securing applications for police, special forces, and government-controlled applications through the combined use of GPS and Galileo. As recalled in this paper, as GPS was already the “reference” for GNSS when Galileo was

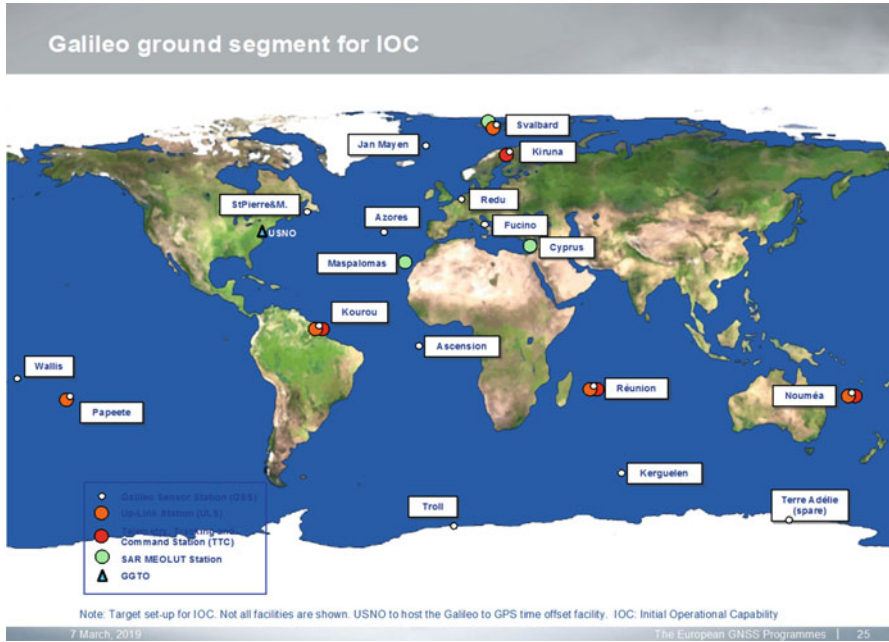


**Fig. 6** Launch of four Galileo satellites with an Ariane 5 launcher (2019) (artist view)

designed, the European GNSS is foreseen to complete the GPS and to be used in complement to improve its safety, integrity, and performances in general. As discussed also previously, for users who access the different open services of the four constellations (GPS, Galileo, BeiDou, and GLONASS), even some secured applications can be foreseen for specific needs (timing for critical infrastructure or secured communications, authentication, even navigation, and positioning, etc.). For each case, a specific threat/vulnerability and risks analysis should be conducted. In particular, the infrastructure plays an important role in the efficiency of the GNSS system as it includes the management of the security incident, the calculation of the ephemerids, or the ionospheric corrections. Such elements help enhance the efficiency for the user at the receiver level.

Here is a high-level scheme of Galileo's ground segment as deployed for initial operational capability (Fig. 7):

Prior to Galileo, Europe's first venture into satellite navigation was the development of EGNOS (European Geostationary Navigation Overlay Service), the European SBAS, and the equivalent of WAAS in the USA. As WAAS does over the US territory, EGNOS improves the performance of GPS over Europe, and, since 2011, EGNOS makes GPS suitable in Europe for safety critical applications such as flying aircraft or navigating ships through narrow channels. It should be noticed that EGNOS's design allows the augmentation in the future of GPS but also other GNSS constellations such as GLONASS or Galileo.



**Fig. 7** High level description of Galileo ground segment for IOC

As a satellite navigation augmentation system, EGNOS includes a network of monitor stations across Europe and beyond that constantly monitor GNSS signals. Thanks to this monitoring functionality, EGNOS is able to correct GNSS orbit and clock estimation errors as well as signal propagation delays through the ionosphere providing a user positioning accuracy within 1–2 meters most of the time, a significant improvement compared to GPS alone, which may stay in the range of about 5 or more meters (depending mostly on ionospheric conditions).

EGNOS also provides verification of the system’s integrity. Integrity is a feature which meets the demands of safety critical applications in sectors such as aviation and maritime, where lives might be endangered if the location signals are incorrect. Integrity mainly relates to the provision of timely warnings when the GNSS system or its data should not be used for navigation. It also gives a measure of trust that can be placed in the correctness of the information supplied by GNSS.

Today, many GNSS receivers available on the market are also EGNOS enabled (Fig. 8).

### Concept of GNSS Interoperability

The UN ICG define GNSS interoperability as the ability of global and regional navigation satellite systems and augmentations and the services they provide to be



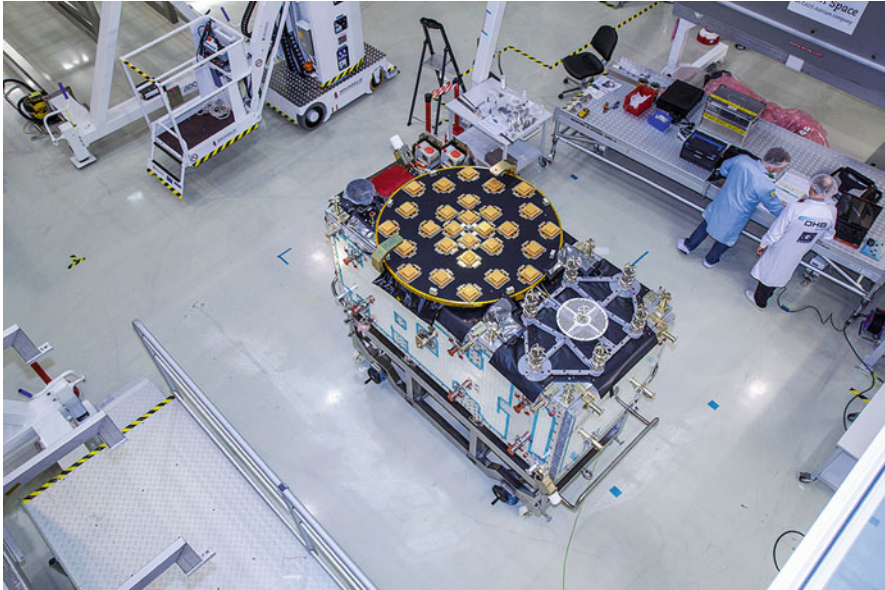
**Fig. 8** Galileo's infrastructure: Ground station in Fucino (Italy)

used together to provide better capabilities at the user level than would be achieved by relying solely on the open signals of one system. In practical terms, it means that:

- Interoperability allows navigation with signals from different systems with minimal additional receiver cost or complexity.
- Multiple constellations broadcasting interoperable open signals will result in improved observed geometry, increasing end user accuracy everywhere and improving service availability in environments where satellite visibility is often obscured such as forests and urban canyons.
- Geodetic reference frame realization and system time steerage standards should adhere to existing international standards to the maximum extent practical.

For a GNSS user, it means that in the future, his device will be able to process four GNSS constellations, not only GPS. These “combined receivers” will allow improved performance as compared to current GPS-only receivers.

The US-EU Agreement on GPS-Galileo Cooperation signed in 2004 laid down the principles for the cooperation activities between the USA and the European Union in the field of satellite navigation (Handbook of Space Security. Policies, Applications and programs 2015). In particular, this cooperation has led to the development of an interoperable and compatible OS signal design for the GPS and Galileo systems, as discussed previously, called the MBOC (multiplexed binary offset carrier) signal. The potential use of this signal by several GNSS is discussed between system providers, bilaterally and multilaterally within the UN ICG (Fig. 9).



**Fig. 9** Galileo's satellite assembly

A joint EU/US report, also derived from the US-EU 2004 agreement (EU-US Cooperation on Satellite Navigation 2010), has demonstrated the benefits of GNSS interoperability by showing the advantages of combining future GPS and Galileo open services. The report demonstrates and quantifies the improvements that can be expected when using GPS and Galileo open services in combination under different environmental conditions. Particularly, in partially obscured environments, where buildings, trees, or terrain block portions of the sky, the combined use of GPS and Galileo often allows a position fix that would have been impossible otherwise with only one system. The benefit of having at least 2 constellations of 30 satellites, meaning an operational use of 60 satellites, or possibly 4 constellations with a total of 120 satellites with secured access is widely recognized by the authorized users to be of a significant operational benefit.

### **Vulnerabilities of GNSS Services**

Because of the increasing reliance of our societies to GNSS, a lot of work (In particular: Vulnerability assessment of the transportation infrastructure relying on the GPS, 29 August 2001, Volpe National Transportation Systems Center and Global Navigation Space Systems: reliance and vulnerabilities, The Royal Academy of Engineering, March 2011) has been done to assess the possible failure modes and vulnerabilities of these types of systems and the potential mitigation techniques.



The vulnerabilities of GNSS can broadly be classified into three main categories:

1. System vulnerabilities, including signals and receivers.
  2. Propagation channel vulnerabilities (atmospheric and multipath) and accidental interference.
  3. Deliberate interference.
- 
1. GNSS have system-level vulnerabilities. For instance, GNSS satellites have on rare occasion broadcasted dangerously incorrect signals, or a reduced number of satellites visible because of a bad geometry could prevent the availability of a position fix, and GNSS receivers can incorrectly process valid signals to give incorrect results. In addition, GNSS signals are very weak, typically less than 50 watts transmitted from a distance of 23,000 km from the Earth. When received at the surface of the Earth, the signal strength may be as low as  $10^{-16}$  watts, with a spectrum spread out effectively around ten times below the noise floor of the receivers.
  2. Furthermore, signals are vulnerable to disruptions in the atmospheric medium they pass through, and receivers can also unintentionally lock onto reflections of the signals, known as multipath, giving unexpectedly large errors. They are also vulnerable to solar eruption and can be disrupted during this phenomenon. This causes can have quite different effects on users, such as partial or complete loss of the positioning and timing service; poorer accuracy; very large jumps in position, velocity, or time; and “hazardously misleading information” (HMI) that is to say, believable data that is dangerously wrong in safety critical applications like civil aviation. The aforementioned SBAS systems (EGNOS, WAAS) are able to detect HMIs related to the GNSS and the ionospheric propagation.
  3. As mentioned supra, the GNSS signal is very weak at the surface of the Earth and can be easily jammed or disturbed internationally. This will be detailed here after.

## **Deliberate Threats to GNSS Services**

Apart from the system-related vulnerabilities (over which the system providers have control), propagation channel errors (which are due to natural effects that can be modeled to some degree but that are by nature difficult to avoid), and accidental interference (which are difficult to anticipate), there are three distinct forms of deliberate man-made interference with GNSS signals: jamming, spoofing, and meaconing. These threats are increasingly worrying the GNSS stakeholders because of their possible safety and security consequences.

Jamming is the most likely threat and could impact the widespread use of the GPS. Jamming devices are radiofrequency transmitters that intentionally block, jam, or interfere with GNSS receivers. Criminal jamming is caused by people who are looking to defeat GNSS tracking systems. They may be car thieves, road toll evaders, and tracker evaders. It is illegal to use GNSS jammers in most countries.

However, in recent years, the number of websites offering “cell jammers” or similar devices designed to block communications and create a “quiet zone” in vehicles, schools, theatres, restaurants, and other places has increased substantially.

Meaconing (delaying and rebroadcasting of GNSS signals) and spoofing (transmission of a false GNSS signal) are more sophisticated and complex types of deliberate interference and therefore are for the time being less common. However, while a spoofer was a very bulky and expensive device some years ago, nowadays, spoofers can be portable and fit into a small box. While jamming intends only to disrupt GNSS service, meaconing and spoofing try to maintain GNSS service but with a false computed position.

The crudest form of jammer simply transmits a noise signal across one or more of the GNSS frequencies, to raise the noise level or overload the receiver circuitry and cause loss of lock. Circuits and assembly instructions for GPS jammers are widely available on the Internet, and commercial jammers can be bought for less than 20 euros. Commercial jammers are sophisticated and cheap: some are designed to fit into a pocket, some into car lighter sockets; most jammers are designed to block GPS, GLONASS, and Galileo. Powerful jammers are also commercially available, up to at least 100 W transmitted power.

There are concepts used in defense, known as NAVWAR (Navigation Warfare). The jammer or the spoofer can be used by military forces in certain areas of conflict, for example, in order to deny GNSS services to non-allies. In this case, only authorized users (allies) are allowed to have access to GNSS services, giving them operational superiority on the field.

One major threat to GNSS signals, even secured ones, is jamming. In this case, there are many ways to improve the performances of the receivers. One of them is to use specific antennas known as CRPA – controlled reception pattern antennas – which are able of digital beam forming and to create a “hole” in the pattern of the antenna in the direction of the jammer to cancel its action. It is de facto one of the best technologies to be used operationally in secured environments. To overcome the above-described potential risks of interference, there are several countermeasures at different stages of the receiver, some of which are mentioned here:

- Noise jamming can be overcome to some degree by CRPA and noise filtering in well-designed receivers.
- The use of two or more antennas can overcome the threat of spoofing by comparing the differential measurements obtained in the antennas with the real ones.
- The front end part of the receiver can incorporate between jamming and spoofing detection methods at the analog to digital conversion (ADC) of the signal, e.g., an indicator called jamming-to-noise ratio ( $J/N$ ) is available in some receivers.
- Inertial measurement units (IMU) can be hybridized with GNSS receivers. Inertial sensors (i.e., accelerometers, gyroscopes, and gyrometers) are not impacted by external radiofrequency emissions and are therefore able to provide a valid position even in the presence of jamming and spoofing, at least for a

certain amount of time. This is probably the most robust countermeasure against the previous listed threats.

The proper combination of these different technologies can be, by design, the best GNSS security solution toward certain needs and in front of certain threats.

---

## **GNSS Applications Relevant for Security**

Space has a strong strategic value. This allows countries to gain independence, scientific and technological prestige, and the capacity to act as a global actor. In fact, the development of space technologies has been often linked to a vision of worldwide strategic posture: that was the case, starting from the 1950s, in the USA, Russia, and France, where launchers and space assets were historically conceived as key elements of nuclear deterrence. But even if nuclear deterrence is put aside, space is synonymous of a whole chain of strategic technologies and activities: from launching to the establishment of satellite telecommunications, observations, meteorology, and navigation, space assets appear as a strategic set of infrastructures, meaning that they cannot be backed up by other types of ground networks and that their disruption would be critical to the whole society. Space assets should therefore be considered as “critical infrastructures,” as their disruption would endanger both civilian and defense activities.

Space applications and technologies are best suited for dealing with an increasingly expanding concept of security. If, on the one hand, traditional customers are military users, on the other hand, a wider security and civilian community can benefit from space services which are being developed. This is particularly true for GNSS. Here are some users identified for some GNSS security applications (Fig. 10):

A critical component of any successful rescue operation is the knowledge of position and time. Knowing the precise location of landmarks, streets, buildings, emergency service resources, and disaster relief sites reduces that time and saves lives in case of natural or man-made disaster or any other type of crisis situation. This information is critical for the disaster relief teams and public safety personnel in order to protect life and reduce property loss. GNSS data (position and time) can contribute in every phase of the disaster management cycle (see the picture below) which is typically composed of three phases: (1) preparedness/prevention, (2) emergency response, and (3) recovery.

## **PMR: A Combined Use of GNSS and TETRA/TETRAPOL (Fig. 11)**

In Europe, just a few companies can offer a European solution for the PMR device of which Airbus and Finmeccanica. In the USA, you can find other devices, such as Motorola. Airbus group has tried to sell its PMR activity in 2017/2018 but has finally kept this secured solution in Europe. The infrastructure of PMR is developed and maintained in Europe by many industrials like Airbus or Nokia, for instance. There



**Fig. 10** PRS potential user communities and applications

are a lot of pressures for the development of the future of these technologies, with the arrival of 5G technology in particular. Huawei has probably invested more than 10 Md€ to develop it, whereas Nokia or Sony Ericsson may have invested around half of that amount. So, the future of the PRS for secured applications (no defense) is closely linked to the future of PMR. We could imagine that the marginal cost of the PRS, when it will be included in the PMR, could be in the order of magnitude of a few euros if included in hundreds of thousands of receivers, for police forces or customs, for example.

For the development of this market, the Commission has the full support of the GSA, the GNSS Security Agency, based in Prague (Czech Republic). This agency has an important role on the market analysis on GNSS and the support of the development of the user segment of GNSS and Galileo and its secured applications in particular. They are clearly key players for the future of secured GNSS and the PRS in particular.

Some specifications for applications require a high level of continuity and availability, in more of the security for the users. For example, rail users are the most stringent community for integrity, even more than aviation; so, some users belonging first to the European Union, may need to use the PRS, as long as their government and organizations have settled the proper organization. For example, the member states who want to use the PRS have to settle a CPA – competent PRS authority. This key authority, usually at a very high level in the states (Presidency in Italy or Prime Minister Services in France – the SGDSN), is responsible of many secured missions and tasks to secure the PRS (Decision 1104/2011 of the European

**Fig. 11** Airbus TH9 Tetra PMR (professional mobile radio)



Parliament and of the Council of 23 October 2011 on the rules for access to the Public regulated Service provided by the GNSS established under the Galileo program.)

Furthermore, the GSA have then conducted an important number of survey and market analysis, published at end of 2018 (GSA 2018a, b, c), of whom I would like to mention:

- a) Report on maritime and inland waterways user needs and requirements (Reference: GSA-MKD-MAR-UREQ-229399, Issue/Revision: 1.0 Date: 18/10/2018) (GSA 2018).
- b) Rail report on user needs and requirements (Reference: GSA-MKD-RL-UREQ-229496, Issue/Revision 1.0, Date: 18/10/2018) (GSA 2018).
- c) Report on time and synchronization user needs and requirements (Reference: GSA-MKD-TS-UREQ-233690, Issue 1.0, Date: 18/10/2018) (for the next paragraph) (GSA 2018).

## **GNSS, Galileo, and Timing for Secured Applications**

In Europe, some member states have conducted studies on their critical infrastructure, to analyze, in particular, the dependency of their infrastructure on GNSS. The

third report of the previous paragraph (report on time and synchronization user needs and requirements), from the GSA, stresses the fact that GNSS is not only strategic for Europe for navigation and positioning but that timing is probably as important as the others! It is key for the member states and for the banking sector to have a proper synchronization of secured telecommunications. For instance, many systems are using encryption and need a perfect synchronization mechanism to encrypt and decrypt signals.

The first discussions and negotiations between the European Commission and the US Department of States (DoS) in the year 2000 were focused on timing. The USA offered to deliver free GPS timing to Galileo. GPS uses a tremendous infrastructure in Washington, with more than 200 atomic clocks (a hundred in the year 2000), connected with Kalman filters and others, to deliver the GPS time. After discussions between the USA and Europe, the technical solution for the benefit of both parties has been that each party gives the other its timing reference. An exchange of the two times references (Galileo and GPS) through a facility called the GGTO – GPS Galileo Time Offset – provides a common reference of timing and significantly improves the resilience and also the performance of the systems. As an improvement, the critical infrastructure such as the PMR or banks, which rely for their timing in many cases on GPS, can easily rely also on Galileo timing and improve their reliability and resilience.

To conclude, the use of GPS and Galileo timing for critical infrastructures or sensitive and secured applications, such as telecommunications, banking, or commercial applications using encryption, is interesting to improve availability and resilience toward some incidents like signal disruptions. As timing is key for these secured applications, the GGTO and the use of at least these two constellations in the receivers improve the resilience of the systems using not only GPS but also GNSS. From an economic point of view, following threat and vulnerabilities analysis, when the use of GNSS is possible, the system designers could avoid using atomic clocks in many cases. Furthermore, there are huge opportunities for developing innovative applications for new developments like Internet of Things (IoT), as soon as the user needs a certain level of security for its assets.

## **The PRS and the Brexit**

It is nearly impossible not to speak about the Brexit as the UK has been an essential contributor to the PRS on the Galileo program in the years 2010–2018. There are at least three major consequences in Europe, on Galileo and its member states, and in particular on the PRS and its secured applications:

- The security of the Galileo constellation is managed by a specific infrastructure called the GSMC – Galileo Security Monitoring Center. The main center is based in France, in Saint-Germain-en-Laye, whereas the backup center was based in NATS infrastructure in South UK, in Swanwick, between Portsmouth and Plymouth. Indeed, the first consequence of the Brexit is that the program has taken the decision to settle the new backup in Spain and to leave Swanwick.

- The second main consequence is that the UK, after the Brexit, would become a third state toward the European Union, as it is for the USA, Norway, or Switzerland, for example. They will have to sign a specific agreement with the European Union to access the PRS. And under the Decision N° 1104/2011, they will not have the same rights as the member states of the European Union.
- Furthermore, inside a PRS receiver, there is a specific module, called a security module (SM) (On the two last generations of military GPS, the PPS – Precise Positioning Service – and the M-Code, there is a similar SM which is called the SAASM – Selective Availability Anti-Spoofing Module. It has been designed in 1998 for some applications requiring protection from jamming or spoofing. SAASM allows satellite authentication, over-the-air rekeying, and contingency recovery.) in which the designer of the receiver hides secured information such as the cryptographic keys to access the PRS and decrypt its navigation messages. Should Brexit happen, the UK industry would not be allowed to build security modules of the PRS receivers (Legal consequence of the Decision N° 1104/2011/ EU of the European Parliament and of the Council of 15 October 2011 on the rules of access to the public regulated service provided by the global navigation satellite system established under the Galileo program (Article 3.5 (b)).).

---

## Conclusions

The revolution is there: about 120 GNSS satellites are in orbit around the Earth and nearly always 15 in view for any user worldwide. From civil to security applications, they give the users a wide array of potential new applications including timing, positioning, and navigation. Careful assessment of the threats and vulnerabilities and the needs of the different security users (police, customs, special forces, etc.) is essential to respond appropriately. For some applications, the users can develop applications relying on the commercial service of Galileo or on the open services of the four constellations, even hybridized with inertial components. In the field of security, the operational advantage of using encrypted GNSS for authorized users, in particular in times of crisis, when open signals can be jammed or spoofed, is huge. For the high level of security required by security users in Europe, the use of the Galileo PRS worldwide seems to be the best option.

**Acknowledgments** Frederic Bastide from the European Commission has contributed to the previous version of this article.

---

## References

- European GNSS Agency (GSA) (2018a) Report on location-based services user needs and requirements outcome of the European GNSS'. Gsa-Mkd-Lbs-Ureq-233604, (1.0)
- European GNSS Agency (GSA) (2018b) Report on maritime and inland waterways user needs and requirements, 1–164. Retrieved from [https://www.gsc-europa.eu/system/files/galileo\\_documents/Maritime-Report-on-User-Needs-and-Requirements-v1.0.pdf](https://www.gsc-europa.eu/system/files/galileo_documents/Maritime-Report-on-User-Needs-and-Requirements-v1.0.pdf)

- European GNSS Agency (GSA) (2018c) Report on rail user needs and requirements outcome of the European GNSS' User Consultation Platform, 80. Retrieved from [https://www.gsc-europa.eu/system/files/galileo\\_documents/Rail-Report-on-User-Needs-and-Requirements-v1.0.pdf](https://www.gsc-europa.eu/system/files/galileo_documents/Rail-Report-on-User-Needs-and-Requirements-v1.0.pdf)
- EU-US Cooperation on Satellite Navigation, Working Group C, COMBINED PERFORMANCES FOR OPEN GPS/Galileo RECEIVERS, July 19, 2010. [www.gps.gov/policy/cooperation/europe/2010/working-group-c/combined-open-GPS-Galileo.pdf](http://www.gps.gov/policy/cooperation/europe/2010/working-group-c/combined-open-GPS-Galileo.pdf)
- Handbook of Space Security. Policies, Applications and programs (2015) Springer. Kai-Uwe Schrogi and others. Volume 2. Part III Space applications and supporting services for security and defense, pp 609–630. Positioning, navigation and timing for security and defense. Jean-Christophe Martin and Frederic Bastide
- Hein GW (Germany), Jérémie Godet (GISS), Jean-Luc Issler (France), Jean-Christophe Martin (European Commission), Rafael Lucas-Rodriguez (European Space Agency) and Tony Pratt (United Kingdom) (2001) The Galileo frequency structure and signal design. Proceeding of ION GPS 2001, Salt Lake City, Sept 2001, pp 1273–1282
- Kaplan ED, Hegarty CJ (2017) Understanding GPS/GNSS: principles and applications, 3rd ed., Artech House Publishers, London, 31 May 2017, p 1064
- Status of Galileo Frequency and Signal Design (2002) Günter W. Hein (Germany), Jérémie Godet (GISS), Jean-Luc Issler (France), Jean-Christophe Martin (European Commission, chairman), Philippe Erhard (European Space Agency), Rafael Lucas-Rodriguez (European Space Agency) and Tony Pratt (United Kingdom) Members of the Galileo Signal Task Force of the European Commission, Brussels
- United States Government Accountability Office, Report to the Subcommittee on National Security and Foreign Affairs, Committee on Oversight and Government Reform, House of Representatives, GLOBAL POSITIONING SYSTEM, Challenges in Sustaining and Upgrading Capabilities Persist, Sept 2010

## Internet Links

- <http://cospas-sarsat.org/>  
[http://ec.europa.eu/growth/sectors/space/galileo\\_en](http://ec.europa.eu/growth/sectors/space/galileo_en)  
<http://www.glonass-center.ru/en/>  
<http://www.insidegnss.com>  
[www.gps.gov/systems/gps](http://www.gps.gov/systems/gps)  
[www.gps.gov/technical/ps/](http://www.gps.gov/technical/ps/)  
[www.gpsworld.com/gnss-system](http://www.gpsworld.com/gnss-system)





Marco Detratti and Ferdinando Dolce

## Contents

Introduction .....	822
History of Space-Based PNT for Defense .....	823
GNSS PNT for Defense Users .....	825
Space-Based PNT Systems Landscape for Defense Users .....	828
GNSS Services and Systems .....	828
Alternative Space-Based PNT .....	829
Modernization of Space-Based Secured PNT Services .....	832
Technologies for Future Defense PNT Solutions .....	833
Multi-constellation Defense GNSS Receivers .....	833
Other PNT Sources .....	836
PNT Superiority Impact on Military Tasks .....	838
Conclusion .....	841
References .....	842

## Abstract

Space-Based Position, Navigation, and Timing (PNT) services were conceived, designed, and developed in response to specific defense capability needs. PNT services are recognized as critical enablers for defense operations and as such must be available with the greatest possible robustness and dependability. Operational advantage of having access to such services is so evident that not only the military but also civilians started to exploit them up to the point that nowadays

---

The contents reported in this chapter reflect the opinions of the authors and do not necessarily reflect the opinions of the respective Agency/Institutions.

---

M. Detratti (✉) · F. Dolce  
European Defence Agency (EDA), Brussels, Belgium  
e-mail: [marco.detratti@eda.europa.eu](mailto:marco.detratti@eda.europa.eu); [ferdinando.dolce@eda.europa.eu](mailto:ferdinando.dolce@eda.europa.eu)

space-based PNT have become a commodity significantly affecting not only defense operations but also the global economy. Threats and attacks to such services are for these reasons increasing, putting at risk the continuous availability required for military operations.

## Introduction

Today, the secure service of the global positioning service (i.e., GPS) provided by the US government is an indispensable part of modern warfare for NATO allies, from strategic decision making or operational planning to the conduct of military operations. Since its conception, the main driver of space-based radio (or Satellite) navigation (nowadays addressed as a whole as Global Navigation Satellite Systems, GNSS) was to ensure that the service they provide could support the widest possible spectrum of military operations on a global scale (Fig. 1).

The general dependence of military tasks from such space services increases the number and typologies of attacks to space systems. From an operational point of view, such ubiquitous GNSS dependency, regardless the service considered (e.g., GPS, Galileo, or others), creates new weaknesses that adversaries could exploit easily and effectively. Indeed, despite their potential and strategic dimension, GNSS signals are vulnerable to several factors:

- Natural effects, such as multipath or ionospheric scintillations
- Signal deformations (GPS ringing phenomenon) and data corruptions, e.g., orbital and clock errors
- Nonintentional interference caused by radio transmitters, mobile communication networks, airborne navigation instruments, etc.
- Intentional interferences such as jamming and spoofing

**Fig. 1** Prototype of 3D positioning system for soldier. (© European Defence Agency)



Within the current scenarios, intentional interference and threats (as well as technologies available to adversaries) are evolving in an extraordinary manner and EU Member States' Armed Forces need to face unprecedented challenges, whether stemming from modern high-tech warfare or more hybrid threats. As threats will continue to evolve quickly, so must PNT-dependent systems and platforms in response. Being able to rely on more secure and resilient PNT services for future operations in congested and contested scenarios is therefore a prerequisite which needs to be fully taken into account in the conception, design, development, and implementation of any PNT solutions for defense users. This has both political and operational consequences, rendering much more critical the identification and assessment of the vulnerabilities that adversaries could exploit.

As a matter of fact, space services and in particular GNSS could be considered, following Gen. von Clausewitz's theories (von Clausewitz 1832), as a center of gravity in the future fifth- or sixth-generation scenarios, where the global scale of future wars could be matched by the global coverage on Earth that only satellite-based services can provide. These considerations lead to multiple consequences and were probably also the basis of recent public political declarations from the EU Commissioner related to the need to start thinking on an EU Space Force (Teffer 2019) in parallel with the development of EU space capabilities such as Galileo, echoing the decision of the Trump Presidency to set up a plan for the creation of an independent US Space Force (Wall 2019).

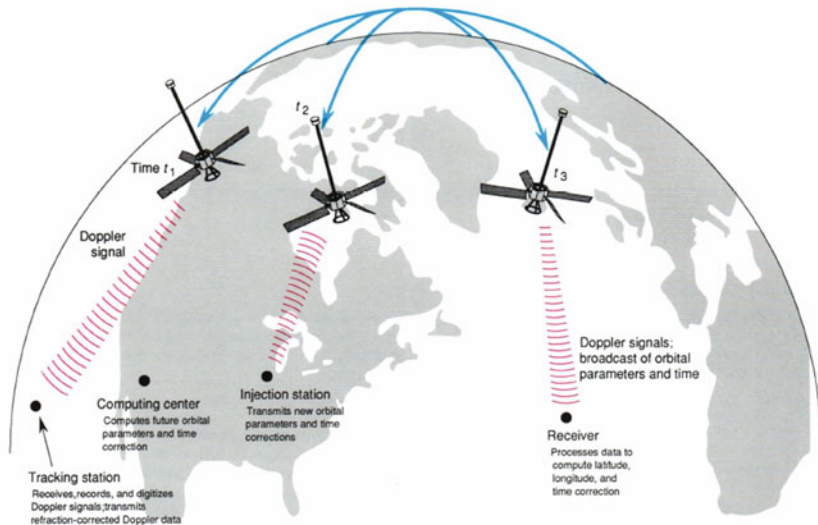
Finally, it is important to underline how, after the transformation of satellite navigation in a commodity, a set of innovative technologies has emerged to improve and complement GNSS in any possible environment and overcome known weaknesses and vulnerabilities. These have to be fully considered and analyzed for the provision of highly robust and dependable PNT services for military forces. Even if GPS was in the driving position (and is going to remain there for a long time to come), PNT is today much more than GPS.

---

## History of Space-Based PNT for Defense

Satellite navigation has its origins in the launch of the first artificial satellite by the Russians, the Sputnik, in 1957. After its launch, scientists in the US Johns Hopkins University discovered in 1958 that, due to the Doppler effect, the radio signals broadcasted by the satellite could be used to localize the satellite. This was used to reverse the problem and exploited to locate an object on the ground based on the knowledge of satellite position.

Based on this idea, in 1959 the U.S. Navy started the development of TRANSIT, the first navigation system to rely on satellites which became fully operational in 1964. Its main scope was to provide position information to the U.S. submarine ballistic missile force. It was not as accurate as today's satellite navigation systems (more than 20 m 2D accuracy, and performance greatly degrading as the speed of the platform increased), but introduced a set of innovations which are the basis of modern GNSS (Fig. 2).



**Fig. 2** The transit concept. (© The Johns Hopkins University Applied Physics Laboratory (Danchik and Lee 1990))

In parallel to TRANSIT development, a study was performed by the Aerospace Corporation for the U.S. Military to analyze tactical applications and utility of improved positioning accuracy. The study concluded with a proposal, in 1966, of satellites relying on highly stable (atomic) clocks to broadcast ranging signals continuously to receivers able to locate moving vehicles anywhere on Earth and in the air on a 24/7 basis. This was the beginning of the satellite navigation system as we know it today. After a series of other technical studies (among which some led to the identification of spread spectrum communication as the best way to transmit the ranging signals), the first four satellites constellation was developed leading to first demonstrations in 1974.

In 1978, the United States Department of Defense (DoD) started the launch of the first operational satellites (even if first Block I satellite with the first on-board atomic clock was launched in 1980) of the Navstar Global Position System, more commonly known as GPS, with the primary purpose to provide Position, Navigation, and Timing (PNT) information to defense users. DoD's primary purpose in developing GPS was to use it in precision weapon delivery, answering to the objectives of the US DoD second-offset strategy. As a second-order objective, such a space-based, all weather, and worldwide available and accurate PNT capability could address the needs of a broad spectrum of applications and would limit the proliferation of specialized PNT equipment supporting specific mission requirements reducing interoperability burdens, hence its almost immediate success.

Despite its early developments, it was only during the 1990s Gulf War (just after the first handheld GPS device for civilian applications, the Magellan NAV1000, was developed) that GPS demonstrated its full potential in operations. GPS navigation

proved to be a crucial force multiplier for desert warfare. GPS satellites, even without a fully functional constellation (in 1991, there were only 19 GPS satellites in orbit, <https://www.af.mil/News/Article-Display/Article/703894/evolution-of-gps-from-desert-storm-to-todays-users/>), enabled forces to navigate, maneuver, and fire with unprecedented accuracy in the desert almost 24 h a day despite difficult conditions – sandstorms, no maps, no vegetative cover, few natural landmarks. GPS’s fully operational capability was achieved in 1995 with the last of the first 27 operational satellites (including the spares) was launched. In the same year, the US DoD, fearing that adversaries could take advantage of the service, decided to decrease the accuracy of the openly available service through the activation of the selective availability.

The importance of this capability has been soon recognized worldwide also for civilian applications, as demonstrated by the development and deployment of other Global Navigation Satellite Systems (GNSS) especially after the end of the Selective Availability in 2000. Since then, GPS-based PNT has deeply changed the way many military operations are conducted by providing (an almost) continuous and ubiquitous precise positioning and timing for a vast variety of platforms at a reduced cost. The trend in the GPS/GNSS device market is not expected to decrease. Instead, it is expected to increase up to US\$2.8 billion by 2027, at a CAGR of more than 2.7% (Market Research 2017). GNSS devices intended for munitions, soldiers, and ground platforms constitute the bulk of defense applications market. These are being acquired either as stand-alone devices or as part of soldier modernization programs. One of the most important factors driving the increase of the market is the fact that new constellations are becoming available and new technological advances are being integrated into PNT systems to increase their robustness by augmenting and complementing space-based capabilities.

---

## **GNSS PNT for Defense Users**

Almost the totality of today’s PNT services rely, either directly or indirectly, on GNSS. Such services are key enabling capabilities in military operations contributing to all the military tasks, fundamental for the freedom of movement and acting as force multipliers. As such, PNT solutions must be secure and resilient. They have to be designed to withstand potential malfunctions and degradations and need to comprise adequate mitigation measures against complex attacks. This is achieved through the concept of PNT superiority against adversaries.

One of the key concepts of PNT superiority is commonly known as NAVWAR (Navigation Warfare). NAVWAR is defined as “the deliberate defensive and offensive action to assure and prevent positioning, navigation and timing information through coordinated employment of space, cyberspace, and electronic warfare. Desired effects are generated through the coordinated employment of components within information operations, space operations, and cyberspace operations, including electronic warfare, space control, space force enhancement, and computer network operations” (US FNP 2017). The underlying benefit of the NAVWAR

doctrine for the military is to ensure military operations PNT superiority and advantage in the area of conflict without disrupting allied forces outside the theater of operations. This is substantially implemented by: “protecting authorized use of GPS; preventing the hostile use of GPS, its augmentations, or any other PNT service; and preserving peaceful civil GPS use outside an area of military operations.”

Since its origin, GPS has become the “gold standard” by which other PNT solutions were (and still are) benchmarked. However, in order to improve the performance of navigation systems in cases of poor satellite coverage and low availability, new GNSS systems are being developed (notably EU is implementing the Galileo program, which is expected to reach full operational capability in 2020). Yet there are still a lot of concerns as space-based services can be denied or degraded in tactical environment; therefore, PNT superiority cannot be limited to NAVWAR. Given the reliance on PNT for operations, the challenge is to maintain a high degree of resilience and the highest possible confidence in any operational scenario even when no external aids to navigation and localization are available.

For the majority of defense forces’ operations, the availability of a globally accurate, precise, and real-time location and timing information can provide a crucial advantage over adversaries. GPS first and other GNSS today are able to provide this capability in many operational conditions allowing, e.g., the effective engagement of opposing forces through accurate targeting, enhanced navigation, and maneuvering activities, and it helps preventing or minimizing collateral damage. This capability is used at several and different military levels such as a strategic analysis, which can take advantage of reliable and global positioning and timing information, or tactical operations, enabling the engagement of high-accuracy weapons’s guidance. This needs to be clearly kept in mind, especially with regard to military rule of engagements that can effectively guide armed forces’ actions and activities.

The revised EDA 2018 Capability Development Plan (CDP 2018) within the 11 identified EU capability priorities clearly reflects the indispensability of space-based communication and information services as an enabler for the defense systems, with a special emphasis on unmanned and autonomous systems (EDM 2018). Unmanned maritime high-end platforms, for instance, which have just been identified as a European priority to achieve maritime surface superiority through long endurance at sea, are only one example where support from space-based applications has become critical. If such systems do not have access to strong and resilient PNT support provided by satellites, they cannot be considered fully operational.

GNSS devices for defense applications are widespread across all operational domains and platforms: soldiers, vehicles, aircrafts, vessels, communications systems, and munitions are routinely equipped with GNSS systems to provide any combination on PNT information. Secure/encrypted GPS receivers for navigation and guidance solutions are available from a handful of manufacturers. Receivers are available either as stand-alone navigation devices or as embedded devices to be operated within a larger mechanical or electronic system.

Space-based PNT services used by European Union Member States and NATO Allies’ armed forces are the US encrypted Precise Positioning System (P(Y) code). Today the de facto user equipment standard is the Defense Advanced GPS Receiver



**Fig. 3** Left: Hand-held micro Defense Advanced GPS Receiver (DAGR). (© Collins Aerospace). Right: TOPSTAR M for avionics platforms. (Photo Thales © E. Raz)

(DAGR) used to provide precision guidance capabilities for vehicular, hand-held, sensor, and gun-laying applications. The latest generation being termed SAASM (Selective Availability Anti-spoof Module) with a quite small and low-weight hand-held form factor for war fighters, with an easy-to-use interface (Graphical User Interface and moving maps). Today there are models resembling conventional smartphone functionalities (including MP3 and camera), but there are several other form factor receivers matching different platform requirements (Fig. 3).

The availability of new GNSS could increase the robustness of the PNT services available to the defense users for the implementation of national or multinational operations. The defense sector should seek to maintain the right level of PNT capability in light of programmatic and technological opportunities and increasing threats to PNT information assurance. Key principles for the usage of space-based PNT solutions (mainly GNSS) as defense-enabling capability can be summarized as follows (ERNP 2018):

- The performance of PNT services in terms of accuracy, continuity, and integrity shall be commensurate to operational needs as defined by Member States in the Capability Development Plan.
- The delivery of PNT services must be subject to agreed governance arrangements and must be under full European control or dependably provided by an allied defense partner.
- Due to the worldwide extent of the EU's area of strategic interests, PNT services must ensure global coverage. Therefore, EU Member States shall have the right to unlimited and uninterrupted access to secured space-based PNT services worldwide.
- The PNT services for military use must ensure a high degree of resilience against all threats and risks; this should explicitly include all aspects of cyber warfare.
- The highest levels of PNT services availability should be sought. Space-based PNT should thus be highly resistant to disruption, denial, deception, and degradation.
- The use of PNT services must be accessible in contested and congested environments.
- It must be possible to deny the exploitation of the secure PNT services by adversary forces.

- Protection and robustness of the equipment must be adapted to the operational environments (e.g., physical security measures, antitampering).
- The interoperability of the PNT services must be ensured in areas of common interest negotiated with GNSS providers.
- The PNT services must be available with a high level of reliability in all operational environments (in particular urban).
- Augmentation systems, regional or local, may be considered in order to enhance available GNSS services.
- PNT services shall be workable from strategic to tactical level, and from the most complex weapon system down to, e.g., dismounted soldiers' equipment.

---

## Space-Based PNT Systems Landscape for Defense Users

Until now, we have been focusing on GNSS as the source of PNT information for military forces. However, as a consequence of the increasing dependency and operational advantages associated to the mastering and control of GNSS systems, several techniques and devices have been developed that can severely degrade the performance of GNSS services. Such degradation, nevertheless, not always causes a complete denial of the service, but most often it causes misleading PNT information (spoofing). Such threats to GNSS might adversely affect various military tasks. In this context, PNT sources and systems can be identified to allow implementing diverse PNT architectures delivering different levels of performance according to the operational scenarios, threats, and missions.

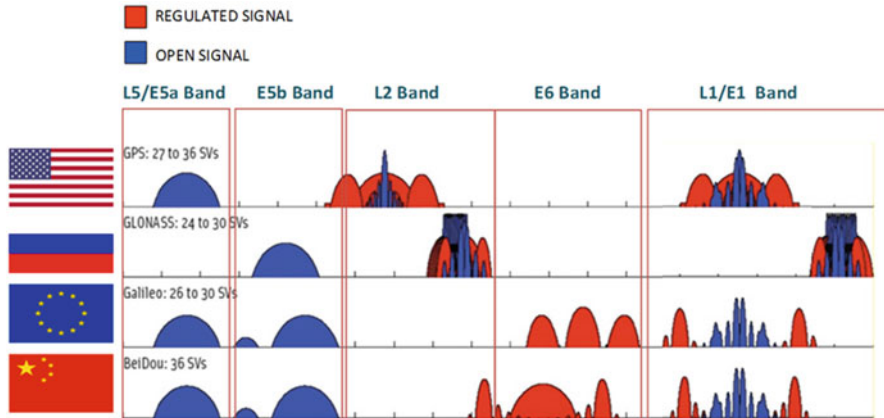
### GNSS Services and Systems

Broadly speaking, two main groups of satellite navigation services can be identified:

- GNSS open services: Provide positioning, velocity, and timing information that can be accessed free of direct user charge. The civilian services are accessible to any user equipped with a receiver, with no authorization required.
- GNSS-regulated and access-controlled services: These are robust services for the provision of PVT (positioning, velocity, and timing) information to authorized users. The regulated signals are typically designed with a focus on the robustness of its signal, which protects it against spoofing and makes it more resistant to jamming.

The only satellite navigation system currently used by military users in EU and allied forces is the US GPS system. However, in addition to GPS, there are three additional satellite navigation constellations in Medium Earth Orbit (MEO): one fully operational (the Russian Glonass), and the other two (the European Galileo and the Chinese BeiDou (BDS) navigation systems) under deployment. The four constellations transmit navigation signals in five different frequency bands featuring both open and regulated services according to the grouping below (Fig. 4).





**Fig. 4** MEO satellite navigation signals (red: regulated signals/services; blue: open signals/services). (Inside GNSS 2013)

In all the aforementioned satellite navigation systems with the exception of the European Galileo, access to regulated (i.e., encrypted) signals is reserved to users authorized by the Ministry of Defense, and therefore mainly targeting military uses and applications. However, albeit being considered and developed as a civil system under civilian control, Galileo will deliver the Public Regulated Service (PRS) which will offer strong and encrypted navigation signals. This secure service is restricted to governmental authorized users and is therefore suitable for services where robustness and complete reliability must be ensured, such as, but not limited to, military operations.

The access to PRS is regulated by Decision No 1104/2011/EU of 25 October 2011. According to it, the PRS is a service which is restricted exclusively to Member States, the Council, the Commission, and the European External Action Service (“EEAS”) and, where appropriate, duly authorized European Union Agencies. It should also be possible for certain third countries and international organizations to become PRS participants through separate agreements. Decision No 1104/2011/EU mentions also that the PRS provide unlimited and uninterrupted service worldwide to PRS participants.

As soon as the Galileo PRS service will become operational, and after the availability of the associated defense user equipment, it could be expected that PRS will become an additional primary source of PNT for EU and allied forces. Indeed, EGNSS could increase resilience, availability, integrity of PNT information, and services for EU CSDP and MS operations.

### Alternative Space-Based PNT

The military use of other satellite navigation services, like space-based augmentation (e.g., WAAS and EGNOS) and their benefit in terms of increased robustness in a

military context is nowadays considered limited. The same applies to civil Differential Global Positioning Systems, RTK, and Post-processing Positioning Services (PPS), especially with respect to the robustness of a military system when relying on such civil augmentation systems. Currently, the main benefit of augmentation in a military context is for aviation applications, with dual-use of the civil system components, like SBAS receivers, and in parallel with military GNSS receivers.

GNSS (GPS, Galileo, Glonass, and Beidou) employ satellites in medium Earth orbit (MEO) broadcasting signals transmitted at an altitude of >20,000 km. This implies about 30 dB more path loss than signals transmitted from LEO satellites (at an altitude of less than 1000 km, like Iridium ([https://en.wikipedia.org/wiki/Iridium\\_satellite\\_constellation](https://en.wikipedia.org/wiki/Iridium_satellite_constellation))). Consequently, with similar transmit power available at the satellite, LEO signals are received at Earth’s surface with a significantly higher power level than GNSS signals. For GPS and Galileo, the observed carrier to noise density ratio (C/N0) in good reception condition is around 50 dBHz, while, e.g., for Iridium, C/N0 values up to 80 dBHz are observed. The higher signal power levels lead to a much stronger jamming resistance of a LEO-based GNSS. Additionally, this allows the LEO signals to penetrate into difficult attenuation environments like deep indoors, where the reception of GPS or Galileo signals is not possible.

Another consequence of the lower altitude of the LEO satellites is a smaller antenna footprint on the Earth’s surface, as illustrated in Fig. 5. In order to have one satellite in view at all times, only around ten MEO satellites are required, while at LEO rather one hundred satellites would be needed. On the other hand, while significantly more LEO satellites are required to provide the same coverage as MEO satellites, launching an LEO satellite is less expensive than launching an MEO satellite.

The lower altitude also leads to a shorter orbital period: for GPS and Galileo, the orbital periods are 12 and 14 h, respectively, while in LEO, the orbital period is around 100 min. Therefore, the LEO satellite geometry, as observed by a user on the Earth, changes much faster than for an MEO GNSS. This has several advantages: the user is observing larger Doppler shifts, which is beneficial for Doppler positioning

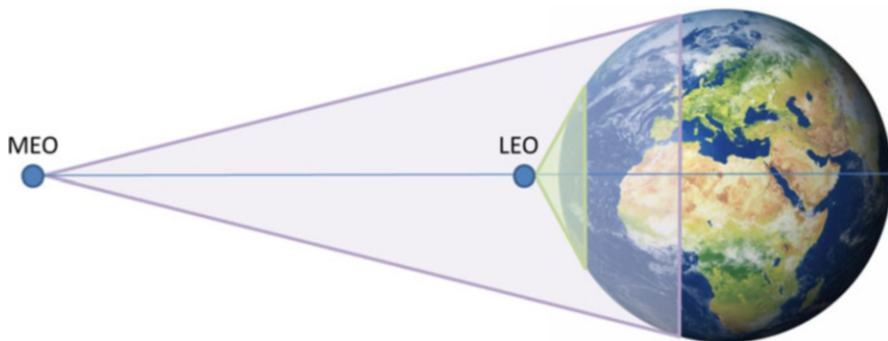


Fig. 5 LEO and MEO antenna footprints on Earth’s surface. (© Reid et al. 2016)

(the same principle used in TRANSIT, see section “[History of Space Based PNT for Defense](#)”). Another positive impact of the fast changing geometry is that it whitens the multipath, which then averages out faster.

Currently, the only LEO constellation with global coverage that offers navigation capabilities is Iridium. Iridium/IridiumNEXT consists of 66 satellites at an altitude of 780 km and is used mainly for communication purposes and is available on a commercial basis. Since May 2016, Iridium offers a Satellite Time and Location (STL) service. Iridium uses overlapping spot beams and randomized broadcasts, which provides a mechanism for location-based authentication that is extremely difficult to spoof (Lawrence et al. 2017). Together with the high signal power levels providing jamming robustness and coverage in deep indoor environments, this antispoofing capability makes Iridium a very robust PNT source. However, Iridium does not yet achieve the accuracy offered by GPS or Galileo. After a convergence time of 10 min, the following performance has been observed in field tests: positioning accuracies between 20 and 35 m ( $1\sigma$ ) and timing accuracy of 0.5 ms.

Even if the performance of Iridium is not comparable with those of the current GNSS, LEO-based PNT is a very dynamic environment, which has the potential for disruptive innovations in the near future that can complement classical GNSS considerably. In the near future, several other LEO-based constellations with possible navigation capabilities can be expected: OneWeb consists of a constellation of 648 satellites for broadband internet provision; the initial operational capability is planned for 2019 (Reid et al. 2016). SpaceX recently got approval from FCC to deploy its satellite internet constellation called Starlink, which adds up to more than 4000 spacecrafts (and up to 12,000) to be operational by the mid-2020s (Ralph 2019). Samsung proposed a LEO constellation of 4600 satellites, and Boeing published plans for a LEO constellation of 3000 satellites (Reid et al. 2018).

Additionally, the U.S. Defense Advanced Research Projects Agency (DARPA) already started to analyze whether military constellations (payloads: global surveillance, tactical communications, and PNT) in low Earth orbit are cheaper and nimbler alternatives to traditional military satellites. In 2017, DARPA launched the project known as Blackjack with the final goal to develop a low Earth orbit constellation to provide global persistent coverage for military operations (Erwin 2018). The project will aim to demonstrate an architecture showing the utility of a global LEO constellation for a wide variety of military payloads and missions.

In a further effort to enhance the PNT capabilities provided by MEO constellations (specifically GPS), the Air Force Research Laboratory (AFRL) in the US will launch in 2022 an experimental satellite in Geostationary orbit (AFRL 2017) called NTS-3 (Navigation Technology Satellite-3) as it follows NTS-1 and NTS-2 launched in 1974 and 1977, respectively, to test initial GPS functionalities). The experimental PNT satellite is intended to test new technologies and hardware to improve robustness and resilience of MEO-based constellations through a supporting layer of geosynchronous Earth orbit satellites. Technologies that will be tested include advanced antenna options, reprogrammable hardware, advanced clock technologies, and new signal structures. NTS 3 will also investigate secured-design technologies to enhance cyber-resilience, as well as modern cyber risks management approaches.

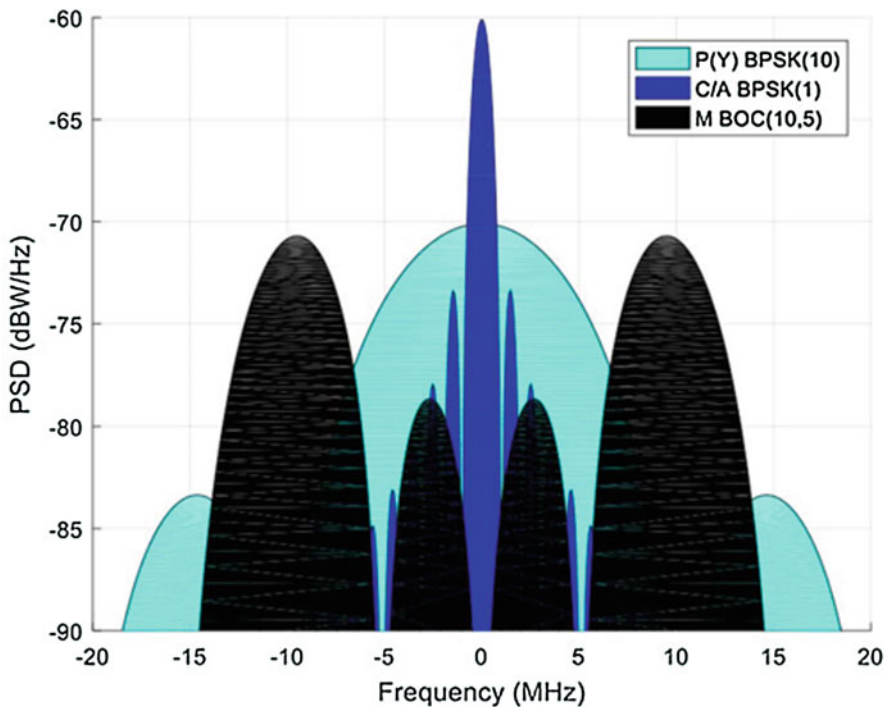
### Modernization of Space-Based Secured PNT Services

In parallel to the completion of the deployment of new GNSS systems and the studies on possible alternative space-based PNT, possibly the most important aspect to be emphasized is the current modernization effort ongoing from US DoD to develop a new secure signal to improve the security features and jamming resistance properties of military navigation using GNSS, the M-code.

The motivations for such modernization can be found in the need to improve NAVWAR performance under the assumption that the threats against the military user (mainly driven by the hybridization of the warfare) are continuously evolving, resulting in an increasingly complex, more congested, and contested environment.

The M-code signal will provide better jamming resistance through much higher power transmission (up to +20 dB above current level, with the possibility through spot-beam transmission to direct the signal toward a specific area of interest) without degrading C/A-code or P(Y)-code reception and in openly available signals on L1 and L2 bands (Fig. 6).

The M-code design also features a more robust signal acquisition, more flexibility in its configuration and better security in terms of exclusivity, authentication, and confidentiality (hence better spoofing resistance), along with a simplified key



**Fig. 6** M-code signal compared to legacy GPS signal around the L1 (1575.42 Mhz) frequency. (© GPSWorld)

distribution (Barker 2000). In particular, the signal is able to support NAVWAR activities: the energy signal is split into two lobes separated from the center frequency, enabling selective jamming of the open GPS (C/A code) without impacting military signal reception (“blue force jamming”). Currently, such blue force jamming is not possible with P(Y) code receivers, without also degrading the friendly force’s receiver.

The M-code is designed to be autonomous, and so authorized users will be able to calculate their positions without requiring the use of other signals (e.g., the C/A-code in the case of the P(Y)), providing at least comparable performance to the P(Y)-code.

To the best of the authors’ knowledge (GMV 2011), also within the Galileo program, in the frame of the design of its second generation (G2G), services are expected to deliver improved performance and features such as reliability, maintainability, availability, continuity, accuracy, and integrity. It is therefore auspicious that PRS performance will be improved in addition, likely to reflect the evolving threat landscape in which defense (a recognized user community of Galileo) will operate.

---

## Technologies for Future Defense PNT Solutions

### Multi-constellation Defense GNSS Receivers

Several techniques and technologies could be used to improve the robustness of GNSS receivers. Based on an analysis of publicly available information (F-DEPNAT), an overview of possible technologies and techniques for use in a military grade GNSS receiver is presented in Table 1.

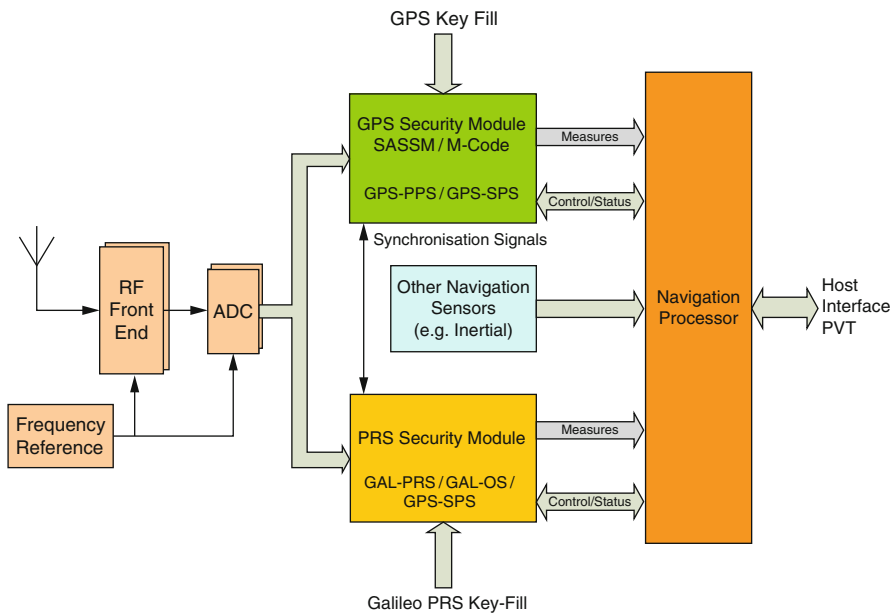
In addition to the usage of multi-frequency (which is the de facto standard for military grade receivers), the use of multiple constellations allows for robust GNSS through improved availability of satellites with good geometry. Use of multiple constellations also mitigates against failure modes associated with a single constellation and supports diversity of signals across constellations and frequencies.

In a military context, the multi-constellation and multi-frequency receivers could make use of different secure, encrypted signals. In addition, a diversity of open signals may be used alongside advanced interference and spoofing mitigations to provide the highest levels of PNT security and robustness for users. For countries in NATO, the use of multiple secure signals will most likely mean GPS-PPS + Galileo PRS. The clear benefits of dual constellation GPS and Galileo receivers for employing encrypted signal services from different constellations are likely the key driver of the requests from United States (Gibbons et al. 2017) and Norway (De Selding 2015) governments to access the Galileo PRS.

Figure 7 illustrates a proposal for a dual mode receiver architecture employing GPS-PPS and Galileo-PRS. This architecture is based on separate security modules to process the encrypted PPS and PRS signals but maximizing the commonality of the remainder of the receiver (e.g., use of common frequency reference subsystem, radio front end). In the figure, a separate navigation processor is shown, but it is potentially feasible for this to be incorporated within one of the security modules.

**Table 1** Technologies and Techniques for Military grade GNSS Receiver

Antenna & RF-Front-end technologies for military-type GNSS receiver	
Antenna type	Chip, helical, patch, choke ring, CRPA beamforming
GNSS bands signals	GPS L1, L2, P(Y), M-code (2020+), E6 PRS, E1 PRS (2020+)
Precorrelation BW	15–40 MHz
Sample quantization	2–8 bits/sample
Sample rate	Up to 200 MHz
Precorrelation RFI detection/suppression	CW, swept CW, notch filter, dynamic chirp filter, pulse suppression
Reference oscillator	TCXO, OCXO, CSAC
Typical implementation (2018) w/o dc/dc converter	Single mini circuit board with 2–3 RF ICs and reference oscillator
Baseband processing techniques for military-type GNSS receiver	
Carrier tracking architecture	FLL-assisted PLL, PLL
Code tracking architecture	Carrier-aided DLL
Multipath mitigation technology	Narrow correlator, multicorrelator
Early-late correlator spacing	0.3–0.01
Other features	Massive parallel correlators for acquisition and tracking, multipath and RFI mitigation, sensor fusion capability
NavSEC/ComSEC	Separate security module for key generation/storage and message demodulation
Typical implementation (2018)	1–2 FPGAs and impeded or separate $\mu$ -processor, tamper protection, key loading module



**Fig. 7** Example of GPS/Galileo dual constellation receiver. (Courtesy of Nigel Davies © QinetiQ)

According to Davies et al. (2016), future challenges to be solved for dual constellation receivers include:

- **Technical:** Even if the development of operational PRS receivers is ongoing in Europe and subject to a number of initiatives, the development of the next generation of GPS-PPS, namely M-code, is more advanced.
- **Security:** There are separate US and European security rules and sensitivities. Therefore, security constraints arise for the key management and handling.
- **Legal/political:** The GPS-PPS security modules can be developed and approved by US contractors under the control of the US DOD and US National Security Agency (NSA). Similarly in Europe, the PRS access rules legislation requires that PRS security modules are developed and manufactured by authorized European manufacturers. Furthermore, use of GPS-PPS outside the US is limited to authorized nations for the purposes of defense under bilateral agreements with the United States.

These points, in addition to the agreement on which military uses could mostly benefit from a combined use of GPS- and Galileo-secured signals and the establishment of the relevant agreements, should be addressed adequately in order to ensure that the defense forces (in addition to the mass and automotive market which are already benefiting from open-service multi-constellation) would be able to fully exploit the benefit of multi-constellation performance.

### **Developments in the United States**

The Military GPS User Equipment (MGUE) program started the development of M-code capable GPS receivers in 2013. According to the MGUE program schedule (Wilson 2015), GB-GRAM-M receiver kits are now available for integration in receiver housing and into military platforms, as shown in Fig. 8. In (Menschner 2018) the GPS enterprise, roadmap is shown for the full system, including also the MGUE Integration and test phases for the various user platforms which are expected to last until 2021.

### **Developments in Europe**

The deployment of the Galileo Public Regulated Service user segment has been steered in recent years actively by the European GNSS Agency (GSA). One essential prerequisite for the future adoption of PRS by multiple user communities is the availability of receivers for different applications. Thereto, GSA has initiated the EU-funded projects P3RS-2 (awarded to an Italian/German consortium, (Leonardo 2014) and PRISMA ((GSA2015, which, based on publicly available information seems being awarded at least to French and German companies) for the development of the first generation of preoperational receivers and first prototypes. In addition to the prototype and proof of concepts developments driven by the GSA, several national development activities are running under the control of national defense agencies and competent PRS authorities. However, information on the expected availability date of the testing and integration of fieldable products are not publicly available.

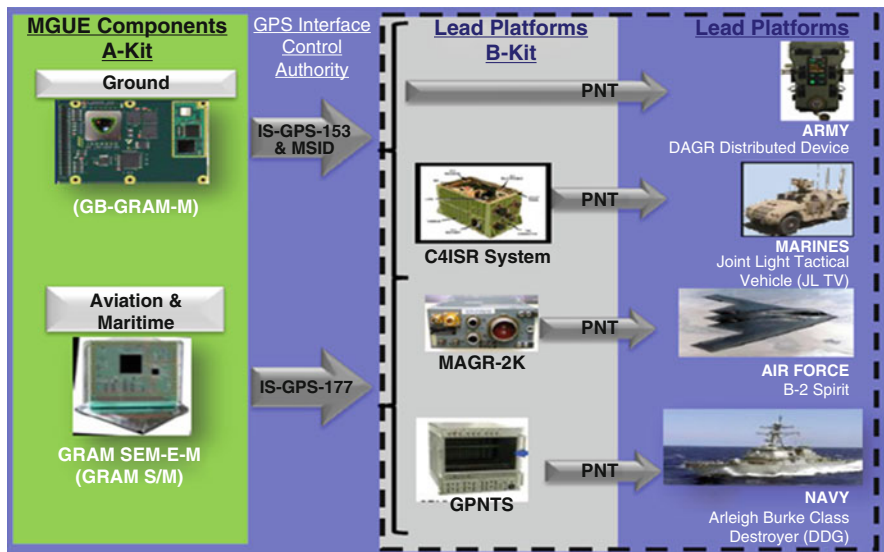


Fig. 8 MGUE Increment 1 M-code receiver development. (© GPS.GOV, Wilson 2015)

### Other PNT Sources

Considering the strategic nature of space-based PNT infrastructures and in order to reap the most benefit from it for critical defense applications, its military potential needs to be recognized and fully understood. On this basis, resilience should be integrated to grant reinforced reliability and dependability to match the growing operational expectations following the evolution of modern warfare. For this reason, and despite not linked with space security, it is important to mention the fact that defense users are currently looking for alternative and autonomous (i.e., not dependent from GNSS or other PNT aids external to the concerned system) PNT sources to assure its continuity under all conditions.

Even if the widespread and worldwide adoption of GNSS in applications which were not even imaginable at its conception have implied the assumption that GNSS PNT is taken for granted, and the GNSS modernization is well underway with the progressive introduction of new constellations and signals, PNT and GNSS are not to be considered synonyms (a quite common mistake nowadays). With a host of technological evolutions on the horizon, PNT is much more than GNSS these days. Other technologies and techniques to augment and complement GNSS need to be studied to ensure PNT superiority to defense forces when GNSS is degraded (or simply not available for physical limitations). This is why several communities (laboratories, research organizations, civilian industry, and others) are being looked at and challenged by defense organizations to propose and explore novel and disruptive solutions. This is of utmost importance also considering the pace at which commercial innovation, without the constraints of traditional defense R&D, are progressing.



In particular, both hybrid and autonomous systems and components would need to be considered. As an example, it will be crucial to develop further Inertial Navigation Systems (INS), traditionally the optimal GNSS complement to guarantee and improve robustness of PNT information in GNSS denied or degraded environments. Work is ongoing to exploit advanced fiber optics (i.e., hollow core), quantum, or micro-PNT technologies (under development under multiple DARPA programs, McCaney 2015) to develop high-performing autonomous (i.e., not depending on external inputs) navigation sensors. In the area of quantum devices, Europe is also progressing with the development of the first commercially available inertial sensors (a quantum gravimeter, Fig. 9). However, current technological status is limited to quite big and static apparatuses with limited dynamic range and high sensitivity to environmental effects. Significant work is needed to develop solutions suitable for compact and dynamic environments and devices able to withstand defense operational and environmental conditions. Integration into defense platforms cannot be expected before 10–20 years.

GNSS evolutions will naturally benefit from related technological advances, some of which will make their signals less susceptible to interference and spoofing (e.g., through the usage of quantum cryptography). It is in fact important not to forget that, thanks to its worldwide availability and attainable cost/performance ratio, it is unlikely that GNSS will be replaced by another technology anytime soon.

Today's trend is in the provision of assured PNT relying on the integration of traditional PNT technology with nontraditional and emerging technology to improve the robustness and dependability of mission-critical applications in all the military



**Fig. 9** First commercially available quantum inertial sensor. (Absolute Quantum Gravimeter, © Muquans, 2019)

operational domains. Fusing different sensor modalities to create a combined navigation solution is anything but a new idea. The benefits of combining GPS with an inertial sensor were recognized a long time ago, and this classic pairing continues to be the subject of research today. In particular, the deep integration produces an increasing of robustness to GPS jamming, compared with tightly coupled systems. However, technologies available to make PNT systems resilient are evolving and nowadays (and in the foreseeable future) a wide range of solutions to match different operational conditions and environments could be imagined.

By combining GNSS-based PNT equipment with detection and mitigation systems, we will continue to rely on trusted GNSS as the main source for PNT services. The combination of several PNT sources can generate different ways to deliver and to use the service. For example, based on the military mission or task, different PNT sources could be selected as main PNT provider, and standard operational procedures could be developed to support the use of different PNT source in case of NAVWAR environment. Such procedures could also be implemented in technical solutions, but in any case need to be flexible and adaptable to the operational tasks and the external threats.

---

## PNT Superiority Impact on Military Tasks

The Generic Military Task List (GMTL) is a taxonomy agreed between EU Member States in the framework of the European Defence Agency to categorize the full spectrum of military activities divided into six domains: command, inform, deploy, engage, protect and sustain. Usually military systems are designed and developed to generate capabilities able to provide services in a subset of the above-mentioned domains.

Several systems can be operated to support one or more of these generic tasks; nevertheless, there are cross-cutting capabilities enabling a very large or, sometimes, the entire spectrum of GMTL tasks. Among those, PNT is one of the most critical and it gives a justification to why PNT superiority needs to be ensured. In Table 2, some examples of how PNT technologies can support the full spectrum of GMTL domains are reported.

**Table 2** Examples of PNT support to military tasks

GMTL domain	PNT support
<b>Command</b>	Time and synchronization for C4I equipment, Blue Force tracking
<b>Inform</b>	Localization of jammers and spoofers, geographical information services
<b>Engage</b>	Mobility and personnel localization, weapons guidance, and precision engagement
<b>Protect</b>	Counter-IED support
<b>Deploy</b>	Platform mobility support
<b>Sustain</b>	Combat search and rescue

Timing sources are crucial for the synchronization and functioning of all networks and digital platforms at strategic, operational, and tactical levels. At tactical level, synchronization enables fundamental capabilities such as effective interoperability, and joint and combined operations that only a globally available service, such as GNSS, can automatically enable for an unlimited amount of users in different locations.

The dependence from PNT services is particularly critical for high precision engagement and missile defense, while a high level of dependence can be assessed for air defense and C4ISTAR services (ItAF 2014). As far as air high precision engagement capabilities, navigation, and guidance of weapons are highly impacted by a PNT-denied environments. As demonstrated by a NATO study (Schmidt 2013) through dedicated simulations, performance of precision-guided munitions can be degraded by a wideband GPS jammer close to the target up to a positioning error 10 times higher than in a noncontested environment. This can lead to catastrophic collateral effects due to the increased circular error probability (CEP), affected, at the same time, also by potential weapons' guidance systems' additional errors due to possible GNSS interferences. For these reason, in some circumstances, due to the rules of engagement, missions might be inexecutable in PNT-denied environments. In order to minimize such risks, air-launched precision-guided weapons, which rely on GPS during the navigation phase, can be complemented by laser inertial gyros to provide a precise guidance close to the target. Furthermore, once the weapon is very close to the target, an infrared receiver on the weapon compare the acquired imagery with the one memorized, providing high-level accuracy guidance in the last phase of the guidance (ItAF 2014).

There are air-launched unguided bombs that can be converted into precision-guided munition through an integrated GPS-aided INS guidance kit to improve the laser seeker and infrared technologies. The bomb could be used also with the laser seeker only; nevertheless, the accuracy degradation when GNSS is not available produces an increase of the target location error which in turn increases the probability of collateral damage (ItAF 2014). Also, as far as missile defense capabilities, there is a strong vulnerability of RADAR systems from GPS positioning information in the C2 management system (ItAF 2014) (Fig. 10).

Examples of these effects have been observed during the Iraq War in 2003, when the Iraqi Army used GNSS jammer to disrupt US GPS-guided missiles (Miles 2004). Several additional reports of GNSS jamming have been published about activities in Iraq and Afghanistan that have undermined military operations since then. Although in many cases such incidents can be quickly controlled in a military environment (they usually rely on a high power jammer which can be easily localized with modern equipment), it underlines the criticality of GNSS and the need not only to exploit space services but also to protect them.

Based on this information, it is clear that the improvement of GNSS services play a fundamental role. For example, the improvement of antijam capability of GNSS services is a clear requirement for military users. With the future generation of GPS Block III satellites, the accuracy of GPS service will increase from 3 m to 30–15 cm and in addition the new M-code in replacement of the current Y-mode will produce

**Fig. 10** Pit drop trials during Joint Direct Attack Munitions (JDAM) integration on Tornado



higher spoofing resilience. Antijamming capability will be increased with the increasing of the signal power, +20 dB above current level, with the possibility to direct the signal toward the area of higher interest.

Several techniques and devices have been developed and new ones will be certainly developed in the future that might severely degrade the performance of GNSS services, ultimately resulting in a complete denial of service, or even worse causing misleading PNT information (deception and spoofing). In particular, GNSS spoofing events have been regularly observed (C4ADS 2019) in the last few years in the Russian Federation, Crimea, and Syria, demonstrating how the military use and development of GNSS threats is growing to pursue tactical and strategic advantages both at home and in foreign territories.

All such threats to GNSS adversely impact various military tasks, such as those described above as some examples. For this reason, PNT superiority integration into military operations and systems is more and more relevant in view of ensuring force superiority in the battlefield of the future. This should be related to the understanding of the relevance of space domain and in particular the PNT sources in military operations. The threat scenario “A day without space,” in fact, reveals a clear dependency (of current and future military operations) on space. At the moment, however, such a threat can be considered as an expression of the soft power (Nye 2005), even if it is clear that in a future strategic prospective the situation will evolve. As defined in “On War” (Von Clausewitz 1832) a center of gravity is “*the source of power that provides moral or physical strength, freedom of action, or will to act,*” and in this sense, the space domain is already moving toward becoming a center of gravity for fifth-generation warfare.

A direct consequence of this qualitative consideration is based on the space threats proliferation that will generate the need to defend the space as a critical infrastructure, strategic nodes, or a military capability.

The real issue is that we are facing threats that were not planned to be dealt with, for technological but also mainly political reasons. Indeed, not only defense equipment is being targeted, but also the entire space segment as witnessed by several developments in this area. A recent report from the office of the Secretary of Defense (USDEF 2019) underlines how China is improving its counterspace capabilities. In addition to directed energy weapons, its antisatellite missile systems (following the tests in 2014) are being further developed. Even if the Chinese government has not acknowledged any specific antisatellite program, there are several publications from defense-funded academies that stress the necessity of “destroying, damaging, and interfering with enemy’s reconnaissance...and communication satellites” suggesting that such systems (and the navigation ones) could be among the targets for attacks. The very recent Indian tests of antisatellite weapons (Foust 2019) as well as the decision to constitute a new military service dedicated to Space Force by U.S. President D. Trump (Wall 2019) are a clear signal toward this direction.

The peaceful use of space (UN 2008) would possibly become a right to defend and not an acquired status relying on international agreements. Space will follow the same path of the sea and air domains, started as a research and development environment when men were not able to navigate or to fly, and then transformed into capability domains to defend from external threats for the benefits of all the civil population. Rather sooner than later, the space domain will evolve to a sphere to be reached before the others, to a source full of enabling services. The above-mentioned recent anti-satellite’s strike capabilities performed as test demonstrators are clear evidence that we need to start preparing to defend space from such kinds of threats.

In this view, the recent declaration of European Commission during the last European Space Policy conference emphasizing the need of start thinking to an EU Space Force (Teffer 2019) in parallel with the development of EU space capabilities, such as Galileo, looks as the product of a defense-oriented Strengths, Weaknesses, Opportunities, and Threats (SWOT) analysis performed in a process of strategic thinking. Indeed, as remarked in the EU Global Strategy, performant and robust PNT services are a key factor to enhance the responsiveness, the credibility, and the responsibility of the EU. In the end, denial or disruption of satellite navigation signals may heavily impact the effectiveness and the capabilities of EU military forces.

---

## Conclusion

The assumption that space-based PNT services will be always and in any conditions guaranteed to EU Member States is debatable and the last EU Space Global Strategy clearly refers to this as a need of strategic autonomy. Such awareness in EU Member States is not homogeneously spread. It could be erroneously considered that GNSS services are a given-capability, even without the standard requirements’ definition process.

Recent events are confirming that space domain is already a congested and competitive domain, where several and new forms of threats will appear, operate, and evolve. PNT services will be affected, and considering the high level of military capability dependency from GNSS, a broader and comprehensive approach needs to be put in place supporting the development of dependable PNT services and sources capable of meeting European defense operational requirements in any of the envisaged scenarios.

All this, coupled with the almost ubiquitous dependency on space-based PNT services, require that defense planners and leaders understand that building more resilient PNT capabilities needs careful thinking and the implementation of architectures that transcend individual PNT-enabled systems, taking into account the need to protect not only the delivery of PNT services to users but also to render the space assets more robust and resilient to new types of threats.

A common definition and agreement of PNT requirements and related concepts of operations aimed to identify primary, alternate, and back PNT sources for defined military scenarios and platforms is indeed a crucial step to guarantee a holistic and robust PNT service to armed forces during military operations.

---

## References

- Air Force Research Laboratory Space Vehicles Directorate (2017) Navigation Technology Satellite-3 (NTS-3). <https://www.kirtland.af.mil/Portals/52/documents/NTS-3-Factsheet.pdf?ver=2017-04-05-140456-050>. Accessed online 12 Apr 2019
- Barker B et al (2000) Overview of the GPS M-Code signal. In: Proceedings of the 2000 national technical meeting of the Institute of Navigation January 26–28, 2000
- C4ADS (2019) Above us only stars. Exposing GPS spoofing in Russia and Syria
- Danchik R, Lee P (1990) The navy navigation satellite system (transit). *J Hopkins APL Tech Dig* vol 11, pp 97–101 (ISSN 0270-5214)
- Davies N et al (2016) QinetiQ, UK, D. Hagan, H. Mayoh, D. Mathews, Rockwell Collins, UK Towards Dual Mode Secured Navigation Using the Galileo Public Regulated Service (PRS) and GPS Precise Positioning Service (PPS), ION 2016
- De Selding P (2015) U.S., Norwegian paths to encrypted Galileo Service Open in 2016. <https://spacenews.com/u-s-norwegian-paths-to-encrypted-galileo-service-open-in-2016/>. Accessed online 12 Apr 2019
- EDA Capability development plan (CDP) (2018). [https://www.eda.europa.eu/docs/default-source/eda-factsheets/2018-06-28-factsheet\\_cdpb020b03fa4d264cfa776ff000087ef0f](https://www.eda.europa.eu/docs/default-source/eda-factsheets/2018-06-28-factsheet_cdpb020b03fa4d264cfa776ff000087ef0f). Accessed online 12 Apr 2019
- EDA European Defence Matters (EDM) (2018) The future needs space, European defence matter issue #16, November 2018
- Erwin S (2018) DARPA to begin new effort to build military constellations in low Earth orbit. [spacenews.com/darpa-to-begin-new-effort-to-build-military-constellations-in-low-earth-orbit](https://spacenews.com/darpa-to-begin-new-effort-to-build-military-constellations-in-low-earth-orbit). Accessed Apr 2019
- European GNSS Agency (2015) PRISMA – Development of low end operational PRS receivers including security modules architectures. <https://www.gsa.europa.eu/prisma-development-low-end-operational-prs-receivers-including-security-modules-architectures>
- European radio Navigation Plan (ERNP) (2018). <http://ec.europa.eu/DocsRoom/documents/33024>. Accessed online 12 Apr 2019

- Foust H (2019) India tests anti-satellite weapon. <https://spacenews.com/india-tests-anti-satellite-weapon/>. Last access 29 Apr 2019
- Future Defence PNT (F-DEPNAT), EDA Procurement procedure 18.CAT.NP3.024. [https://eda.europa.eu/procurement-biz/procurement/eda-procurement/18.cat.np3.024%2D%2Dfuture-defence-pnt-\(f-depnat\)](https://eda.europa.eu/procurement-biz/procurement/eda-procurement/18.cat.np3.024%2D%2Dfuture-defence-pnt-(f-depnat))
- Gibbons G, Inside GNSS et al (2017) Delay continues for effort to add Galileo signal to U.S. Military receivers. <https://insidengss.com/delay-continues-for-effort-to-add-galileo-signal-to-u-s-military-receivers/>. Accessed online 12 Apr 2019
- GMV (2011) Galileo future and evolutions, Navipedia. [https://gssc.esa.int/navipedia/index.php/Galileo\\_Future\\_and\\_Evolutions](https://gssc.esa.int/navipedia/index.php/Galileo_Future_and_Evolutions)
- Inside GNSS (2013) Something old something new. <https://insidengss.com/something-old-something-new/>. Accessed online 12 Apr 2019
- Italian Air Force (IAF) (2014) Spazio a support delle capacita' operative dell'Aeronautica Militare: Dipendenze, Vulnerabilita e Mitigazioni. Italian Air Force Publication, February 2014
- Lawrence et al Innovation from LEO, GPS World, 30th June 2017
- Leonardo (2014) Selex ES-led consortium wins €10.3M contract to hook EU governments up to Galileo satellite's secure navigation signals. <https://www.leonardocompany.com/press-release-detail/-/detail/pioneer-ii>
- Market Research (2017) Global Military GPS-GNSS Devices Market 2017–2027. <https://www.marketresearch.com/Strategic-Defence-Intelligence-v3944/Global-Military-GPS-GNSS-Devices-11068926/>. Accessed online 12 Apr 2019
- Mccaney K (2015) DOD puts emphasis on navigation warfare, accurate GPS signals, [Defensesystems.com/articles/2015/02/09/dod-directive-navigation-warfare-pnt-tools](https://www.defensesystems.com/articles/2015/02/09/dod-directive-navigation-warfare-pnt-tools)
- Menschner A (2018) GPS/PNT modernization progress: state of GPS III, MGUE, accelerating M-code, and resilient PNT, national space-based positioning, navigation, and timing advisory board meeting, May 2018
- Miles D (2004) Iraq jamming incident underscores lessons about space. <https://archive.defense.gov/news/newsarticle.aspx?id=25298>. Accessed Apr 2019
- Nye J (2005) Soft power: the means to success in world politics. PublicAffairs, New York
- Ralph E. SpaceX Starlink becomes first US mega-constellation to gain FCC approval. <https://www.teslarati.com/spacex-starlink-gains-fcc-approval/>. Accessed online 12 Apr 2019
- Reid T et al (2016) Satellite navigation from low earth orbit. SCNPT symposium 2016. [http://web.stanford.edu/group/scpnt/pnt/PNT16/2016\\_Presentation\\_Files/S11-Reid.pdf](http://web.stanford.edu/group/scpnt/pnt/PNT16/2016_Presentation_Files/S11-Reid.pdf). Accessed online 12 Apr 2019
- Reid T et al (2018) Broadband LEO constellations for navigation. *J Navig* 65(2):205–220
- Schmidt G (2013) Navigation sensors and systems in GNSS degraded and denied environments. NATO STO-EN-SET-197 2013
- Teffer P (2019) EU commissioner floats idea for European space force, available through EU Observer. <https://euobserver.com/foreign/143981>. Accessed online 12 Apr 2019
- U.S. Department of Defense, Department of Homeland Security, and Department of Transportation (2017) Federal radio Navigation plan (FRP) 2017. <https://www.navcen.uscg.gov/pdf/FederalRadioNavigationPlan2017.pdf>. Accessed online 12 Apr 2019
- United Nations (UN) (2008) Treaties and Principle on Outer Spaces. New York. United Nations Publications. (ISBN 978-92-1-101164-7)
- US Office of the Secretary of Defense (2019) Military and security developments involving the People's Republic of China, annual report to congress 2019
- Von Clausewitz C (1832) On War, Revised edition with Introduction and Notes by Col. F.N. Maude. London. Kegan Paul, Trench, Trubner & C., 1918
- Wall M (2019) Trump signs directive to create a military space force (Space Policy Directive-4). <https://www.space.com/president-trump-space-force-directive.html>. Accessed online 3 May 2019
- Wilson J (2015) Military GPS User Equipment (MGUE), Lt Col J. Wilson, 29 Apr 2015. <https://www.gps.gov/multimedia/presentations/2015/04/partnership/wilson.pdf>. Accessed online 12 Apr 2019



# Space Traffic Management Through Environment Capacity

# 44

Stijn Lemmens and Francesca Letizia

## Contents

Introduction .....	846
Current Global Actions Undertaken to Preserve the Space Environment .....	848
The Limits of Space Debris Mitigation as We Know It and Beyond .....	855
Towards an Environment Capacity .....	857
Applications Related to Environment Capacity .....	862
Conclusions .....	863
References .....	864

## Abstract

Access to space is in principle regulated by international and national law. Once in orbit, however, the notion of national boundaries is not sufficient for space traffic management concepts as the physical reality dictates that actions of a single object in orbit has consequences on all its orbital neighbors. The space environment is therefore a limited shared resource, i.e., the ability to safely conduct operations. Based on reviewing the limitations of the current space debris mitigation guidelines, a natural extension is proposed by considering the capacity of the space environment to withstand risks associated with resource usage. To achieve this link, a metric capturing the resource consumption of an object in terms of collision risk induced on orbital neighbors is constructed. The integral risk over all actors in orbit is then used to quantify the notion of harmful interference with the environment. Managing this integral risk, i.e., the

---

S. Lemmens (✉)

Space Debris Office, European Space Agency (ESA) – European Space Operations Centre (ESOC), Darmstadt, Germany

e-mail: [stijn.lemmens@esa.int](mailto:stijn.lemmens@esa.int)

F. Letizia

Space Debris Office, IMS Space Consultancy at Space Debris Office, European Space Agency (ESA) – European Space Operations Centre (ESOC), Darmstadt, Germany

e-mail: [francesca.letizia@esa.int](mailto:francesca.letizia@esa.int)



environmental capacity, in the same way as is done for other resources linked with orbits, e.g., frequencies, leads to a dynamical framework for achieving space safety and security through space traffic management.

---

## Introduction

The Introduction section will be used to briefly lay out the international legal and policy regime to deal with environmental issues such as space debris. The following section will describe the current global status in adhering to space debris mitigation guidelines put forward during the last decade, and highlight the various risks associated with both ignoring and adhering to them. The third section will go beyond the current guideline and introduce how a dynamics risk estimate, accounting for the design and operations of a space missions, naturally extends space debris mitigation and leads to the notion of the capacity of the space environment which can be managed as a natural resource in analogy with radio frequencies. The last two chapters mention some further applications and wrap-up with conclusions.

Space traffic management as a concept is not new. Various international fora, e.g., the International Institute for Space Law or the United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS), have been discussing questions such as “how access to space should be regulated,” “what are the rules of the road in orbit,” or “how to integrate launch atmospheric re-entry traffic with air traffic” under various guises and with increased relevance since the 1990s. What has been an increased driver in the debate since the last decade is the focus on safety and security aspects, and the need to get the terminology agreed at international level. For the purpose of this work, the following definition of *space traffic management* is used: “The set of technical and regulatory provisions for promoting safe access into outer space, operations in outer space and returns from outer space to Earth free from physical or radio-frequency interference” (International Academy of Astronautics 2006), focusing on the physical interference.

Under the internationally widely adopted 1967 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (the “Outer Space Treaty”) (United Nations 1966), and further derived treaties such as the 1972 Convention on International Liability for Damage Caused by Space Objects (the “Liability Convention”) and 1975 Convention on Registration of Objects Launched into Outer Space (the “Registration Convention”), it is clarified that access to space is regulated at the State level, with only the common understanding of how to behave in orbit being laid out in those treaties themselves. In absence of fully internationally endorsed follow-on work, how the on-orbit behavior of actors can be made compatible with global safety and security objectives, it is important to recall the two main “hooks” that are available from a space traffic management perspective within the Outer Space Treaty, with a focus on environmental concerns. In particular, when it comes to what nowadays could be perceived as environmental concerns, the treaty does not offer a clear set of

rights or obligations beyond Articles III and IX. The former concerns the need for State Parties, and hence the national actors for which they are responsible, to be acting in accordance to international law. The latter concerns the need of activities in space to avoid harmful contamination, which is one of the main purposes of space traffic management as defined for this work as well.

The currently most pressing environmental issue in outer space is the issue of how to deal with space debris, i.e., the nonfunctional objects of human origin left behind in orbit after six decades of spaceflight which carry the risk of, through collisions among themselves, creating orbital regions where space debris is so dense that spaceflight is impossible (Kessler and Cour-Palais 1978). The risk of triggering this so-called *Kessler syndrome* is in essence a long-term risk. Studies that drive technical guidelines to avoid this fate generally focus on long-term simulations covering spaceflight activities 50–200 years into the future (Inter-agency Space Debris Coordination Committee 2007). However, there are already consequences of our limited stewardship of the space environment that present themselves to present day operators as ever-increasing short-term risks. In certain regions of Low Earth Orbit (LEO) and in the Geostationary ring, having a collision avoidance procedure in place and regularly exercising it has become a common practice. These short-term risks have been mostly caused by fragments from explosions of nonpassivated objects, left in orbit since the start of spaceflight activities, but collisions between space debris objects, including an active satellite with an intact abandoned satellite, have also occurred (European Space Agency 2019). Most recently, also near-term risks in the space environment have become apparent as actors in orbit start adapting to a congested space environment, due to regulations or out of self-interest. For example, a well-known space debris mitigation practice is limiting the orbital lifetime of a satellite to 25-years after the mission has ended. In the last 5 years, the increased adoption of this practice, combined with increased launch traffic into LEO of satellites without maneuver capability, has shown a build-up of object density around 600 km of geodetic altitude, which needs to be accounted for by objects passing through this region.

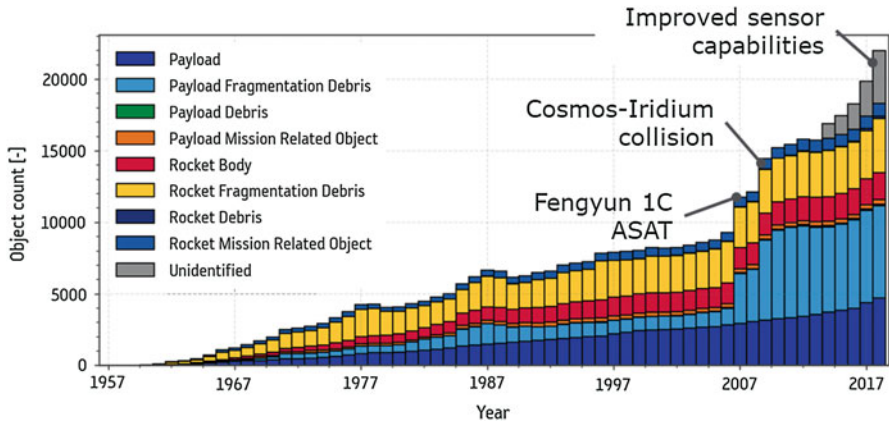
In order to address, among others, the issues posed by space debris on spaceflight activities, UNCOPUOS has taken the initiative to create a set of internationally agreed guidelines for the long-term sustainability (LTS) of outer space activities (United Nations 2019a). These guidelines contain recommendations on the policy and regulatory frameworks for space activities, the safety of space operations, rules of engagement for international cooperation, capacity-building and awareness, and scientific and technical research and development, but omitted security aspects. Under the assumption of an orbit, or orbital region, as a limited and shared resource, a contribution to space traffic management can be made by introducing concepts of top-down resource management compatible with the sustainability guidelines. At the hearth of this will be the quantification of the physical interference that spacecraft and launch vehicles, or collection of those as part of a single mission in the case of larger constellations, can have on the space environment itself and other operators.

## Current Global Actions Undertaken to Preserve the Space Environment

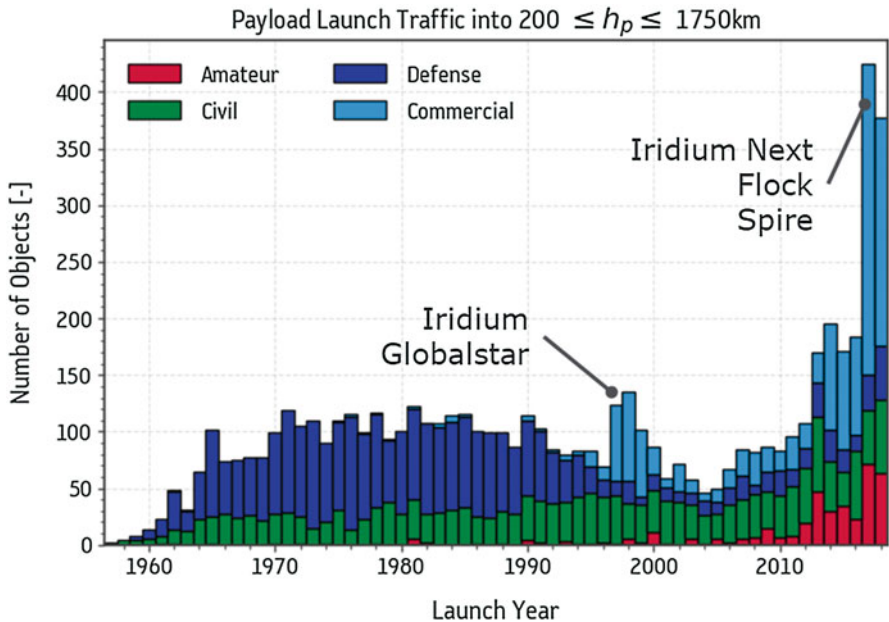
Ever since the start of the space age, there has been more space debris in orbit than operational satellites. As space debris poses a problem for the near-Earth environment on a global scale, only a globally supported solution can be the answer. This creates the need for a set of internationally accepted space debris mitigation measures, in addition to national standards and license processes. A major step in this direction was taken in 2002, when the Inter-Agency Debris Committee (IADC) published its Space Debris Mitigation Guidelines (Inter-agency Space Debris Coordination Committee 2007). This document has since served as a baseline for nonbinding policy documents, national legislation, and as a starting point for the derivation of technical standards. The standardization of mitigation measures is important in order to achieve a common understanding of the required tasks leading to transparent and comparable processes. Even if a consistent set of measures is paramount to tackle the global problem of space debris, it is then up to the individual nations, operators, and manufacturers to implement them. The status of these national activities have been well documented by UNCOPUOS showing the increased uptake within its Member States (United Nations 2019b). In response to the LTS guidelines and its standardization role, the European Space Agency (ESA) publishes a supporting report to provide a transparent overview of global space activities, estimate the impact of these activities on the space environment, and quantify the effect of internationally endorsed mitigation measures aimed at improving the sustainability of space flight (European Space Agency 2019). In the spirit of transparency, this section is based on a recap of the cited report, in the public domain, with permission of the authors.

In more than 60 years of space activities, more than 5800 launches have resulted in more 44,000 tracked objects in orbit, of which more than 20,000 remain in space and are regularly tracked by the surveillance networks around the globe. About 26% of these so-called *catalogued objects* are satellites, or *Payloads*, and only a small fraction, about 2000, are still operational satellites today. About 17% of the catalogued objects are spent upper stages and mission-related objects such as launch adapters and lens covers. More than half of the population is made by fragments generated by more 500 breakups occurred in space, with the two major fragmentation events clearly visible as jumps in the population as shown in Fig. 1. Import to note is that the number of objects reflects the improvement in the capability of the space surveillance systems. When new objects are detected due to increased sensor performance, they can generally not be traced back any longer to an event or source and a growing category of “Unidentified” objects appear in the figure. This has legal repercussions, as there can be damage caused by well tracked and established space debris objects, for which an owner and hence a launching state cannot be identified.

To understand the active interest in space traffic management around the globe, one only has to note the remarkable change in the launch in traffic in Low Earth Orbit, both in terms of volume as in terms of actors, as shown in Fig. 2. The number of payloads has now reached four times the level of 10 years ago, with a steep



**Fig. 1** Evolution of number of objects in geocentric orbit by object class. (With permission of the European Space Agency ©)



**Fig. 2** Evolution of the launch traffic near LEO per mission funding. (With permission of the European Space Agency ©)

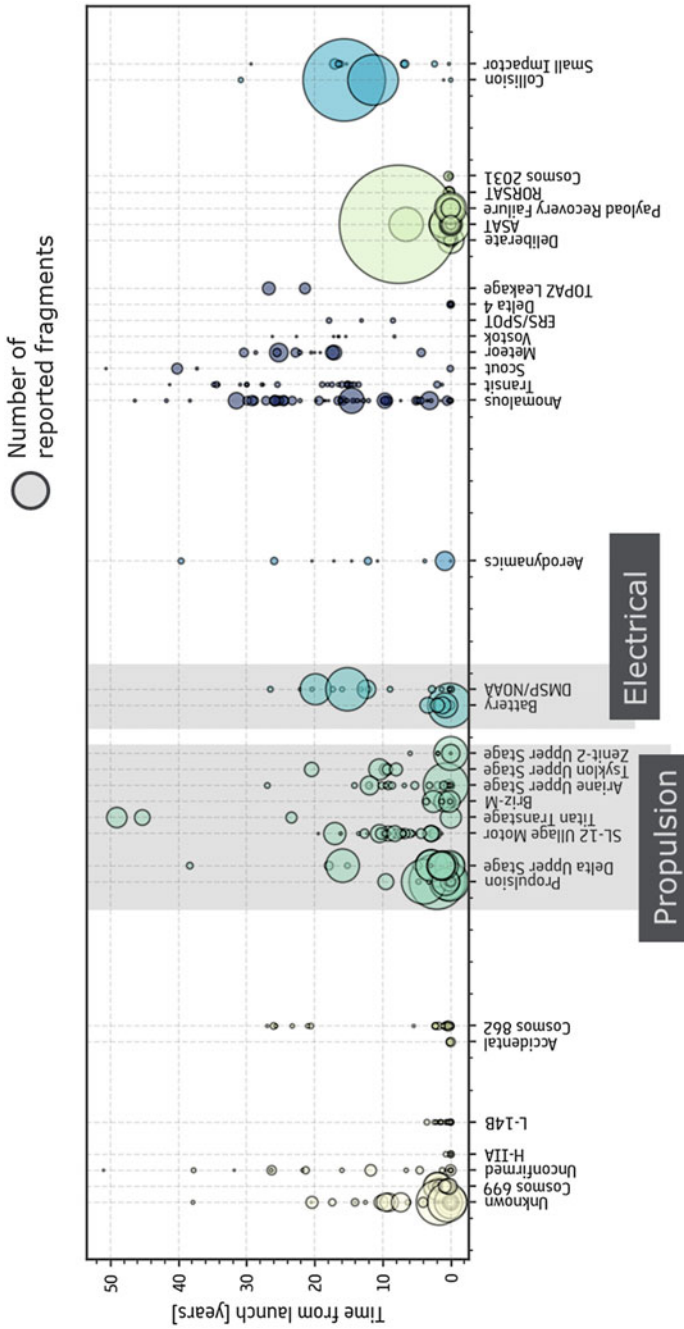
increase in particular since 2017. This growth in numbers is driven by the launch of ever smaller satellites, with around half of the satellites launched in the last 3 years having a mass smaller than 10 kg. This change in traffic is also related to a shift towards a more commercial exploitation of LEO and a diversification in the actors on stage. In 2019 alone, 180 satellites were injected in LEO as part of either the

Starlink, OneWeb, PlanetLabs, or Spire constellation. This number is expected to double in 2020. A similar trend was observed in GEO many decades ago and there it leads to collaboration among the different actors to ensure an effective exploitation of the available orbital slots. Similarly, in LEO, new collaborations among operators may emerge, as more and more operators take an active role in promoting best practices to limit the proliferation of space debris. Collaborations between some operators themselves is likely not sufficient, as the density of operations in LEO would imply that any operator can be affected. A global space traffic management system to coordinate these exchanged would be most efficient.

Counting and identifying launches and objects, and detecting and cataloguing space debris are needed to understand the global use of the environment. In a congested environment, equally important are the development of metrics that serve as proxies for the global adherence to space debris mitigation guidelines which have been put in place to protect the space environment from adverse effects such as the Kessler syndrome. These metrics, such as disposal strategies per object type or breakup events by underlying cause, consider both the historical evolution and the different performance achieved by different class of spacecraft. However, a caveat is that the analysis of the real progress made in the last years in terms of the compliance to space debris mitigation guidelines only appears after the operational life of a satellite. Hence the observed change in the traffic so far implies that in the future the signal could be dominated by the performance of large constellations.

As pointed out in the Introduction, the current short-term risk levels are dominated on-orbit breakups. Guidelines are clear: the potential for breakup should be minimized both during operational phases (for example, by a careful analysis of the failure trees) and after the end-of-mission, by releasing stored energy on-board, as the one in tanks and batteries. Intentional destruction and other harmful activities should also be avoided. Currently, on average 8 nondeliberate breakup events occur per year and this number has not improved in the recent years. One third of the events are related to failures in the propulsion system of the spacecraft. Even if the more systematic application of passivation strategies has contributed to reduce slightly this type of breakups, failures of the propulsion and of the electrical systems still represent a significant contribution to the population of fragments observed in Earth orbits.

It is well known that the distribution of these breakup events is not uniform across the population of objects in orbit, but rather some specific designs have exhibited over the time a higher tendency to fragment. This is particularly evident from the distribution of events by cause and by the time between launch and breakup. For “Anomalous” events, i.e., the separation at low speed of fragments from a parent object, the time appears to be rather uniformly distributed, whereas for certain classes of propulsion and electrical failures, the breakups are clustered around specific times, as show in Fig. 3. Design flaws can appear at different epochs from launch, but, for breakups in space, a higher incidence is observed during the first phase of operations, with half of the events occurring within 16 months from launch. This suggests that for the proposed large constellations operating at high altitude, where a repeating design is fundamental to the cost-model, the risk of breakups can



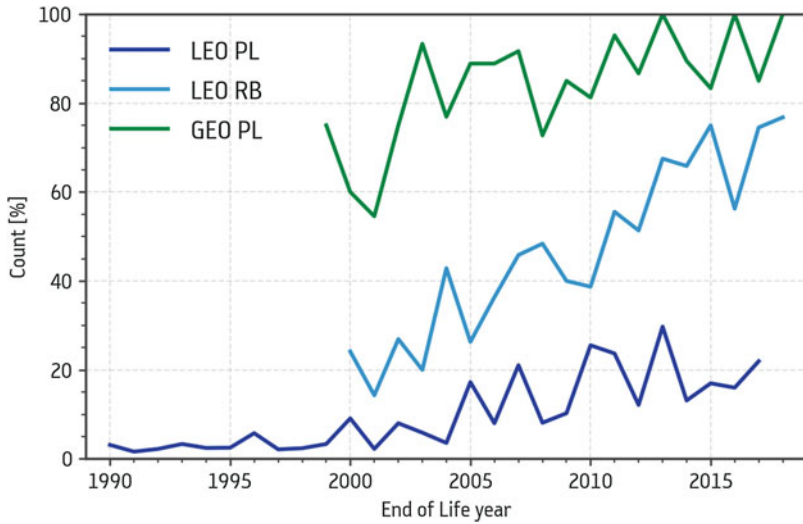
**Fig. 3** Distribution of fragmentation events by estimated cause and elapsed time between launch and break-up. (With permission of the European Space Agency ©)

be mitigated by testing the system at lower orbits before moving to their operational orbit (Inter-agency Space Debris Coordination Committee 2017).

Whereas breakups in orbit are the current dominant source of space debris, the Kessler Syndrome implies that in the future this role would be taken by on-orbit collisions. The probability that these occur is essentially a function of the objects left behind on-orbit. As a mitigation measure, post-mission disposal guidelines have been formulated for two so-called *protected regions* defined by IADC, i.e., the Low Earth Orbit (LEO) and the Geostationary Orbit (GEO). Historically, these regions represent orbits where most operational spacecraft resides and where the collision probability is higher. These regions are protected because of their unique nature, which means that it is important to ensure access and operability in these regions for future missions and this requires defining their sustainable use with respect to debris generation. As mentioned in the Introduction, for objects in LEO, the recommended action is to accelerate their orbital decay such that their permanence in the protected region is limited to at most 25 years after the end of mission; for objects in GEO, it is recommended to move any spacecraft to a disposal orbit sufficiently above the GEO region and rocket bodies into orbits which don't intersect with it in the long term.

Disposal plans and their expected success rate are currently not systematically shared by operators but thanks to space surveillance data, the activity of a spacecraft can be derived and the orbital evolution predicted (► Chap. 50, “Space Object Behavior Quantification and Assessment for Space Security”). This creates a transparent estimate on the behavioral state of any object, free from most biases, which could occur when considering intelligence sources. For objects in LEO, the residual orbital lifetime is estimated and compared to the 25 years mentioned in the guidelines. In this way, one can classify a spacecraft as compliant or not. For GEO objects, the orbital evolution over 100 years is checked to detect any return to the GEO protected region from the orbit where the spacecraft was disposed. In the LEO region, roughly 40% of the total number of payloads operate in orbits that naturally adhere to the space debris mitigation measures, i.e., they will re-enter in the Earth's atmosphere within 25 years from the end of their mission. In particular, around 78% of small payloads, i.e., below 10 kg in mass, operate in such regions. This means that still 22% of these spacecrafts are left in in potentially crowded orbital regions, without any maneuver capability.

For the objects that operate in non-naturally compliant regions in LEO, a low level of compliance is observed, with only around 15–25% of the payloads that have reached end-of-life during the 2010s attempting to comply with the space debris mitigation measures. This class of objects represents roughly 50% of the objects in LEO and around 60% of the total mass in LEO. They can become large contributors to a Kessler syndrome because of their mass (and so the number of fragments that they can generate) and because of their altitude (which results in a long residual lifetime). More optimistically, Fig. 4 shows that shift towards higher compliance rates is possible and already happening for rocket bodies in LEO. While around the year 2000, the attempts of disposal accounted to less than 20%, currently a value close to 80% is reached. Even better performances are reached in GEO, where the

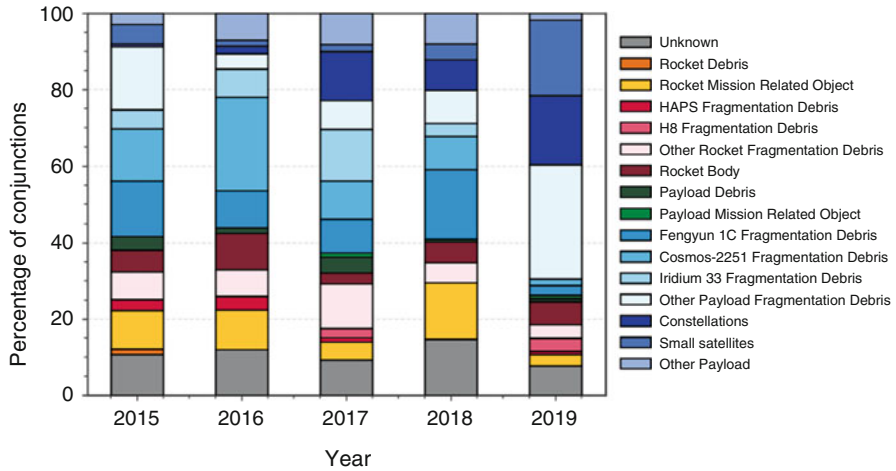


**Fig. 4** Disposal attempt rate for non-naturally compliant objects such as Payloads/Satellites (PL) and launch vehicles/rocket bodies (RB) from the protected regions. (With permission of the European Space Agency ©)

disposal attempts have been consistently above the 80% level in the recent years. The case of GEO, where there is a clear commercial interest in keeping the operational orbits free from defunct or interference causing satellites, has a parallel for large constellations that will also have a similar interest in keeping their orbits clean. In case a collision, failure, or breakup occurs in a densely populated orbital region, the first operators to notice are the orbital neighbors that will have to adapt their procedures. In case of large constellations or GEO operators, these operators tend to form part of the same entity.

Whereas breakups and post-mission disposal address the long-term risk to the space environment, short- and near-term risk associated with space debris mitigation and environment congestion can be captured as well. The changing scenarios in terms of traffic and constellations has an impact on the operation of satellites that can be measured in terms of close approaches. As an experiment, one can assess the close approaches for ESA's fleet of satellites at lower orbits, i.e., below the congested debris regions, and note for these missions an increasing contribution coming from intact satellites in Fig. 5. Such intact, and in some cases operational, satellites include those belonging to constellations and general small satellites (mass lower than 15 kg). This trend, nearly certain to further increase, pushes operators to reconsider their current setup for the collision avoidance activities. Where a piece of debris is involved, collision avoidance processes only require the support of a space surveillance network to track, estimate, and predict the location of the chaser for a risk assessment. On the other hand, in case of operational chaser satellites, in addition also coordination is required to check their maneuverability status and whether any





**Fig. 5** Close approaches for ESA missions at low altitude LEO with various classes of chaser objects (both actively controlled as well as inactive). (With permission of the European Space Agency ©)

collision avoidance plan is in place on the other side. Manual coordination is no longer an option when considering a scenario with thousands additional operational satellites crossing operational orbits of others. There can be very valid reasons for doing such crossings, e.g., when performing a launch and early operations phase in orbits close to the Earth which are not debris dense before raising the orbit to the operational regime at 1200 km of geodetic altitude such as planned for the One-Web constellation in response to space debris mitigation actions (Inter-agency Space Debris Coordination Committee 2017).

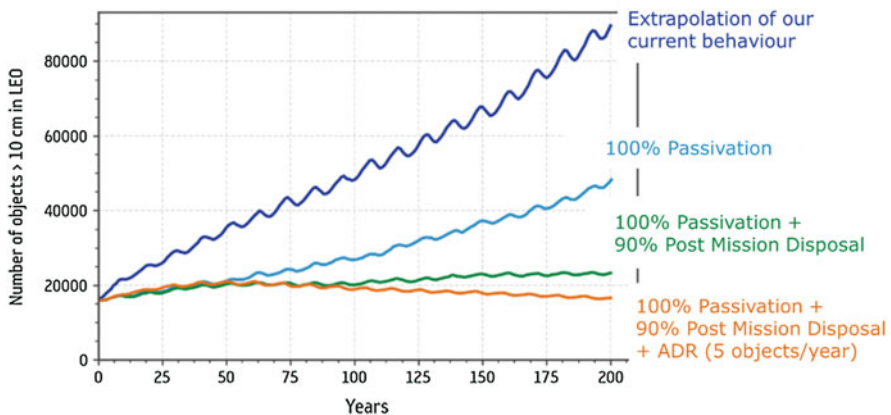
A first step to ease the coordination among operators is to promote data sharing, for example, for what concerns the maneuverability of an object and its predicted ephemerides. A second step is to develop more automated systems for collision avoidance (Bastida Virgili et al. 2019). It is estimated that nowadays global satellite operators spend 14 million euro annually on debris impact avoidance maneuvers, but more than 99% of the conjunction notifications are false alerts. The changing scenarios, in terms of launch traffic, associated to small satellites and large constellations and in terms of improvements in the sensor capabilities, will generate a much larger number of collision warnings to deal with. The introduction of automated systems is not the final solution to the issue of collision avoidance, especially in the cases mentioned before where other operational satellites are involved, but it has the potential to ease the effort required for operations. More effective protocols for timely communication are needed in the future, also to ensure a smooth interaction between automated systems and systems with human in the loop, together with a set of well and unambiguously defined, and standardized, space traffic rules, including transparency in terms of the risk accepted by operators and on how reaction thresholds are defined.

## The Limits of Space Debris Mitigation as We Know It and Beyond

In the previous Section, the state of the space environment and how to mitigate the adverse effects of space debris in the long- and short-term have been described. Many of the mitigation guidelines and standards in place world-wide have been based on the IADC guidelines (Inter-agency Space Debris Coordination Committee 2007), first released in 2002, which in turn were based on best practices available in its member agencies. The effectiveness of those guidelines was derived from space environment projection models. Such models define space traffic scenarios and on-orbit behavior to make a stochastic prediction on the evolution of the space debris environment. As a result of this process, the members of the IADC found that the 25-year post-mission disposal (PMD) rule was suited to reasonably bound the growth of object numbers provided that it has a high adoption and implementation rate.

Numerous studies of the long-term evolution by means of independent space environment projection models demonstrated that addressing breakups and post-mission disposals dramatically affects the growth rate of the debris population. For example, Fig. 6 shows the population of objects larger than 10 cm in LEO over 200 years. In the case where the current trends in terms of breakups and disposal continue are extrapolated to the future, an increase of more than three times in the number objects is predicted. The successful passivation of any spacecraft would already halve the final number of objects. If also a rate of 90% in the successful implementation of post-mission disposal is achieved, the increase of the number of objects over 200 years is only 30%.

This is an example of how, according to several consistent studies on the long-term evolution of the environment, the current level of compliance is not sustainable, in the sense that, if the same level is maintained also in the future, an exponential



**Fig. 6** Example predicted long-term evolution of the environment in different mitigation scenarios, under launch traffic conditions as observed during the 2000's as function of space debris mitigation scenarios including Active Debris Removal (ADR). (With permission of the European Space Agency ©)

growth of the population of objects is predicted, regular collisions will occur, and the associated consequences will be present in everyday operations. International standards and policy call for at least 90% success in post-mission disposal rates, and at most a 1 in 1000 change of accidental breakup (International Standards Organisation 2019). These target values are very far from, respectively, the observed 15% and 8-per-year events previously mentioned, so an important shift in how to deal with this sustainability target is still needed.

For reasons of practicality in view of implementation on national levels, all widely used guidelines and standards address space objects individually. This allows a convenient direct relationship between regulator and an individual space object, and leads to verifiable design targets such as the 25-year rule and 90% post-mission disposal success rate. However, the limitation of performing space debris mitigation in this way is the implicit dependency on a certain underlying space traffic (management) scenario assumed to guide effectiveness of the guidelines. For example, in the case when also the presence of large constellations in LEO are considered in analyses such as Fig. 6, the studies carried out within the IADC have shown how a reasonably stable evolution (but growing) of the environment is achieved only in the cases where not only the disposal success rate is at least 90%, but specifically for constellation objects is at least 95%. The 25-year post-mission disposal guideline can cope with drastic variations of space-traffic as long as it is almost perfectly adhered to (Inter-agency Space Debris Coordination Committee 2017), but technical systems will suffer from failures and a fulfilment of this guideline with a success rate of 100% is not achievable unless the object are inserted in orbits that is compliant to orbital lifetimes from the start. As noted earlier, this however creates a near term risk in form of an orbital shell around 600 km of geodetic altitude, which needs to be crossed by other operational satellites on the way up or down.

At latest with the start of the design of large constellations in LEO, it became clear that the space traffic has deviated dramatically from the assumptions made 20 years ago and space debris mitigation based on the one-requirement-fits-all-objects approach has reached its limits. On the other hand, it also serves to demonstrate the point that the space environment can de facto be seen as a limited shared resource, where the resource is the ability to conduct space operations, with interference being caused by the creation of debris that has to be mitigated. Indeed, considering the classical example for this type of interference one thinks of an object exploding or colliding in an Earth orbit: fragments will reach orbits that are 10s or 100 s of kilometers away in semi-major axis and quickly imply the need of regular collision avoidance maneuvers for the entire region affected once the fragments have been catalogued. A far larger amount of the debris created in this event will not be catalogued and can hence not be avoided, but will still have enough energy in a collision to affect the survivability rate of missions operating in this orbit (Krag et al. 2017). Less classically, releasing a constellation of 100 s of satellites without maneuvers capability in the space environment has environmentally the same effect as a cloud of tracked space debris and implies the same collision avoidance burden on nearby actors, but without the risk associated to undetected objects. The latter example is, however, more commonly interpreted as a space traffic management

issue, but the interference nonetheless caused is the same as what is targeted by space debris mitigation.

To bridge the divide, it is of importance to establish a quantitative metric to describe the risk of interference a space object posed to the space environment, based on its physical characteristics only and in such a way that it can be integrated. A metric constructed in this way can capture the notion of resource consumption and hence quantifies the notions of harmful interference and damage as known from other global environmental issues. The stakeholder situation is diverse, as in absence of a comprehensive international legal regime to deal with space debris, various technical agencies, operators, and other stakeholder fora have been established which deal with recommending and enabling technical solutions to mitigate the proliferation of space debris (International Standards Organisation 2019) and to implement methods of exchange among actors in the space environment (The Consultative Committee for Space Data Systems 2013). The existence of standards and technical mechanisms to deal space debris have given rise to soft law practices by requiring space debris mitigation aspects to be considered as part of a national launch request (Tapio and Soucek 2019). To overcome this, the focus on using physical, or observable, parameters only for the quantification of the interference is importance to avoid misinterpretations. Indeed, as demonstrated by (United Nations 2019b), national regulators can also have different methodologies in tackling space debris mitigation. However, once in orbit the notion of national boundaries should no longer be the sole inspiration for space traffic management concepts as the physical reality dictates that actions of a single object in orbit has consequences on all its orbital neighbors.

When considering the “avoiding interference” part of space traffic management, an extension of the practice of space debris mitigation are on needs to address resource consumption questions such as “Which loss-of-mission risk is placed on other operators due to the behavior of a given mission?” and “What is the contribution of a given mission to the Kessler syndrome?”.

---

## **Towards an Environment Capacity**

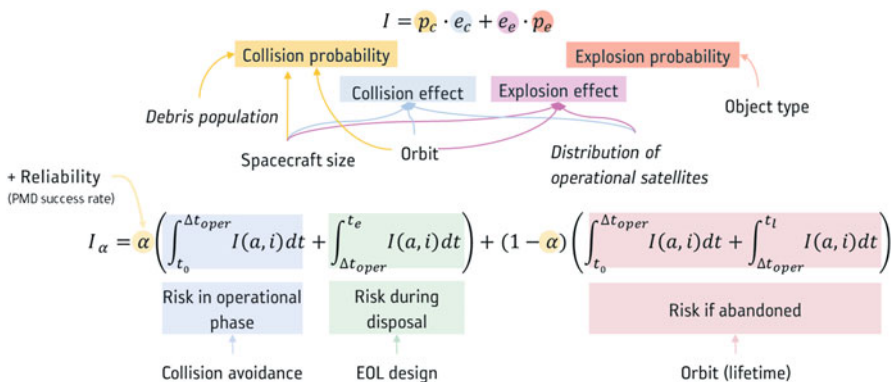
As laid out in the previous sections, a quantification of the interference caused by an object in orbit to the space environment at large is required to bring the methods employed in defining space debris mitigation guidelines to the level of space traffic management. If successful, space traffic management in itself can contribute to a safe environment by strengthening existing space debris mitigation guidelines and requirements based on the actual interference levels in certain orbital regions.

Various attempts have been undertaken by many authors to formulate numerically what the impact is of an object on the space environment. Such approaches range from classical risk, i.e., probability times severity, analyses (Letizia et al. 2016) to purely environmental formulations based on modelling (Rossi et al. 2015), i.e., the likelihood of increasing the amount of objects in orbit. In general, the most simple approach, and common denominator among many said quantifications, describes in

one way or another the impact of an object by the number of fragments released when involved in a collision or breakup (Utzmann et al. 2012). Considering these fragments, combined with the time they will remain on orbits gives a first quantification of how relevant an event is. Further extensions include accounting for feedback effects, i.e., accounting for the interaction of the released fragments with the existing environment (Letizia et al. 2019a), as having a fragment on orbit for a long lifetime is not necessarily a large issue if it has no probability of colliding with other object. In any case, the probability of an object to collide or breakup can be quantified as well and should be accounted for when quantifying interference, to avoid overly conservative estimates.

One metric has been developed for this use case: an index called Environmental Consequences of Orbital Breakups (ECOB) (Letizia et al. 2017). ECOB takes the form of a risk term, i.e., the severity of an event occurring multiplied by the likelihood of the event occurring. The form is shown in Fig. 7 and the main characteristics, relevant in this work, summarized below.

- The severity is assessed by simulating the fragmentation of the object studied and the effect thereof is measured in terms of the resulting collision probability for a set of targets representative of the operational satellites.
- This fragmentation can be due to collision or accidental breakup, with different probabilities and distinct fragments simulated in each case.
- The set of operational satellites in orbit change over time, and hence, the risk is a dynamical estimate, which can be reassessed when the space traffic conditions change.
- The state of the space debris environment at the moment of analysis is accounted for as part of the probability of collisional breakup for the object analyzed and the severity term is a proxy for the increased risk of collision for entire environment at



**Fig. 7** Definition of the ingredients for metric underlying the risk quantification (EOL: End-Of-Life; PMD: Post-Mission Disposal). (With permission of the European Space Agency ©) (Letizia et al. 2017)

large. As such, the combined term is a proxy for the risk of triggering a local Kessler syndrome.

- The formulation accounts for mass, on-orbit exposed area, orbital ephemeris, and regime for a mission, the post-mission disposal and collision avoidance strategies, as well as the operations of the launch vehicle that brought the mission in orbit. Both for the object being evaluated as for other active missions in orbit.

There is also no need to limit the notion of ECOB to single object, as the results can be easily integrated over a group of object such as satellite and its launch vehicle, or a large constellation, or a satellite and objects intentionally released thereof, etc. The word *mission* is used to indicate an evaluation in such generality. The ECOB metric enables us to capture the three different risk perspectives of an object when interacting with the space environment at different time scales:

1. Short-term effect. The severity term is based on the effect of the potential breakup that a spacecraft or launch vehicles upper stage has on its orbital neighbors. On one hand, this includes the risk increase due to fragmentation debris on other active missions, but the ECOB of these other active missions can also be recalculated when a new mission is added to the environment and hence get a feedback on how the operational and disposal procedures would need to change to remain at the same level as without the additional mission.
2. Mid-term effect. Space debris policy measures can trigger behavioral changes of actors in the environment. E.g., the introduction of the 25-year PMD rule implies that nowadays favorable launch insertion is below this boundary, i.e., between 550 km and 650 km of geodetic altitude. By regularly updating the space debris environment model, as well as the representative list of active satellites, the ECOB formulation of environmental impact is dynamic and captures the changes in space traffic that take place.
3. Long-term effect. A risk formulation in terms of the feedback effect a collision or breakup in orbit has on other operational spacecraft is a proxy for the effect on the environment at large, which is currently still dominated by debris objects. As such, the integral risk over the population yields information on the status of the environment at large, and the triggering of the Kessler syndrome will show up as an environmental risk increase.

*Environment capacity* is defined as the term for resource usage of the space environment as quantified by the integral over all ECOB values of objects in the space environment that implies a sustainable future. There are various ways of defining a sustainable future scenario, e.g., ranging for those in which a net reduction in amount of space debris above a given size threshold is envisaged to those in which a maximum amount of yearly collision maneuvers is a given. Such environment trends, as computed by space environment projection models, can be evaluated in terms of their environment capacity, just like any individual mission would, and this value is set as maximum which can be in reality added to the environment across a period of time, e.g., a year. One natural candidate for a predicted future environment

trend to follow comes easily to mind: one that consumes the same environment capacity as those predicted under the strict interpretation and application of the IADC space debris mitigation guidelines. The reason to base ourselves on an existing reference already applied to space debris mitigation is simply that the IADC guidelines have been demonstrated to be robust when adhered to stringently. The level of stringency required, e.g., in terms of postmission disposal success rate or accidental breakup probability tolerated, to follow the trend is automatically determined by the environment capacity to be achieved. A simplified example of how this environment capacity would practically work was played out for the first time in (Krag et al. 2018), with risk simply defined as the sum over all objects released into the environment as part of an event times their orbital lifetimes rather than ECOB.

The notion of thinking of a risk metric which determines the technical and operational constraints of a space mission, including the orbits it can access, is even less novel than the notion of space traffic management itself. In fact, the International Telecommunication Union's (ITU) constitution, which takes the form of an international treaty, via the radio regulation notes in Article 44 that *"In using frequency bands for radio services, Members shall bear in mind that radio frequencies and any associated orbits, including the geostationary-satellite orbit, are limited natural resources and that they must be used rationally, efficiently and economically, in conformity with the provisions of the Radio Regulations, so that countries or groups of countries may have equitable access to those orbits and frequencies, taking into account the special needs of the developing countries and the geographical situation of particular countries"* (International Telecommunication Union 2016). In case of the ITU and the frequencies they manage, the notion of harmful interference is the physical interference caused by electromagnetic waves within similar bandwidths which could render unambiguous reception and decoding of multiple signals impossible. Such interference can be predicted once the design and operational concept is known for a satellite, the interference determines how physically close the beams of satellite can be (e.g., in GEO orbits for telecommunication satellites, accounting for the fact they can go rogue), and the interference is easy to measure once it occurs in practice. Analogously and respectively, ECOB gives the risk of interference with the space environment based on the design and operational concept of a mission, the quantified risk can be used as an actionable value to decide if certain strategies are sustainable (e.g., how close can two large constellations operate together without causing collisions), and space surveillance networks track the on-orbit behavior of objects (including collisions and explosions).

A relevant overview of the full ITU process in this context can be found in ► [Chap. 51, "Space Security and Frequency Management."](#) In Table 1, a comparison is made between the legal regimes, broadly interpreted, that manage the frequency bands available as a resource and those in place for orbits as a resource. For the latter it is important to note that nowhere outside the ITU Constitution orbits as identified as such, and the Outer Space Treaty and common practices presented in this work indicate this. Nonetheless, it is clear that the commonalities with the far more regulated ITU

**Table 1** Top-level differences between the legal regimes responsible for the management of the frequency and orbit resources

ITU constitution and regulations	Outer space treaty
ITU Constitution (Article 44): Radio frequencies and satellite orbits are limited natural resources	Outer space free for exploitation and use by all States Parties in conformity with international regulations;
The ITU Constitution creates, by means of an international treaty, an entire international body with regulatory capabilities. Implementation is a competence of the State Parties	States retain jurisdiction and control over objects they have launched into outer space
Regulations require a rational, efficient, economical use and equitable access	States Parties shall conduct exploration so as to avoid their harmful contamination and . . . and, where necessary, shall adopt appropriate measures for this purpose
Radio waves do not stop at national borders (Laws of physics)	Fragments of an in-orbit breakup will not respect already occupied orbits (Laws of physics)
Interference-free is operations in the purpose of the Radio Regulations treaty	Interference free operations is the purpose of space debris mitigation policies
Allocation, power limits, and equitable use are achieved by clear rights and obligations: <ul style="list-style-type: none"> <li>• Planning (block allocation)</li> <li>• Coordination (first come first serve)</li> </ul>	Current level of international space traffic management is limited to: <ul style="list-style-type: none"> <li>• Best effort coordination between operators,</li> <li>• “Soft Law” alignment across State on space debris mitigation</li> </ul>

processes fall naturally into place with space traffic management when the notions of physical and radio-frequency interference are used as equivalences.

An example can be played out based on a top-down space traffic management framework modelled on the ITU with the physical interference defined as in this section. Most controversial could be the notion that orbits are then allocated based on the design and orbital parameters of a mission, and what can be accounted for in any given year. It is important to note that such an access to space policy based on environment capacity does not prohibit access to certain orbital regions per se. It might however imply stricter design requirements, e.g., a higher reliability on the mechanisms associated with post-mission disposal or a reduced orbital lifetime after the mission well below 25 years (Letizia et al. 2019a). The equivalent under ITU regulations, i.e., block allocation, can, in contrast, effectively block entire bands of the frequency spectrum for certain users. In practice, space traffic management based on environment capacity would imply the need for a simple scheduling and monitoring process:

1. Mission proposals need to be collected before launch with mission descriptions and planning in line with what is currently expected of Space Debris Mitigation Plans (SDMP, International Standards Organisation 2019). This ensures that the planning of available and consumed environment capacity can be monitored at short- and mid-term scales. This is analogous to the national and international coordination of frequency allocation for planned missions.



2. As the available capacity would be linked to a sustainable reference evolution of the environment, e.g., under hypothetical strict adherence to the IADC mitigation guidelines, there needs to be a limited time window in which proposals can be evaluated, in order to ensure that events happening in the environment can be accounted for, and orbits not blocked indefinitely. The book-keeping of capacity allocation implies that ECOB's severity and probability terms can be regularly recomputed to track (planned) changes in the space environment. This is a common practice in planning-based resource management.
3. On a first-come-first-serve proposal-based system, if the capacity of a given launch year is nearly reached, more stringent design criteria would be required to achieve early launch or else an allocation would be postponed. Under-utilized environment capacity would become available in later years.

Technically, the implementation of such a space traffic management system could be as simple as a secure but open access web-based interface, which is synchronized with the ITU registry and linked with a credible and technical international body to ensure accurate modelling of the space environment. The same issues the ITU faces in terms of having reliable input in future behavior would, however, need to be tackled as well. A transparent space surveillance capability to validate that plans are executed as allocated is indispensable as well, e.g., to extend the analysis of ongoing mitigation efforts such as shown in the previous section. Regulatory-wise, the implementation would not be complex per se. Indeed, as regulation currently targets enshrining mitigation requirements either by law, standards, or guidelines on the level of individual missions, and since current requirements need to remain active, this environment capacity approach could just be accomplished by an additional requirement. This additional requirement should ask to demonstrate that the space object fits within the overall capacity apportionment for the envisaged launch year, accounting for both its operational and disposal phase.

---

## Applications Related to Environment Capacity

The notion of environment capacity is based on a quantified risk assessment that needs to be minimized. As this risk, i.e., the ECOB metric, is based on the design and operational concepts of a mission, it can effectively be used as design optimization tool for the sustainability of a mission as well (Letizia et al. 2019b). Among others, this allows the optimal space debris mitigation technology to be defined for various mission classes and orbital regimes. The concept can even be taken one step further, as working with quantified figures also enables new ways of benefiting from active debris removal activities or general trading schemes. E.g., an operator can opt to remove one of its previously abandoned satellites to increase its environment capacity allocation, or operators can trade unused allocation in case their mission performs more sustainable than planned.

At a practical level, the metrics to assess the impact of an object on the space environment have been included into larger environmentally oriented activities.

Transparent and procedure-based evaluations of space missions such as those described in the previous section can be included in life cycle assessments (Maury et al. 2019). Moreover, they have been adopted as an enabling component for a Space Sustainability Rating (Rathnasabapathya et al. 2019), aiming to positively identify those actors in orbit which take extra steps towards space sustainability beyond what is required by national regulations and space debris mitigation standards.

---

## Conclusions

The access to space is currently regulated at the state level under the rules laid down in the outer space treaty, which over the years implied that states and international organizations adopted space debris mitigation policies, which have been based on internationally well-established technical recommendations such as the IADC guidelines. The latter one is, however, a nonbinding legal instrument which can become applicable in law once a state adopts a derived technical standard, e.g., as part of a license to launch process. While such an update into legal regimes is an ongoing process, it is already clear that the global adherence to these guidelines, which were based on space traffic scenarios observed in the 1990s and 2000s, is currently not sufficient to achieve a sustainable space environment. With the recent advent of new actors in the space flight domain, and rapidly changing space traffic scenarios, these guidelines have also reached their limitations in applicability.

Space traffic management, when being based on the concept of avoiding physical interference which would be detrimental to actors in orbit and the space environment at large, offers a natural regime to put in place a top-down approach where orbits are considered as a limited shared resource and allocation is based on a quantified risk metric. To this end, a qualified risk estimator such as ECOB that captures the notion of the risk incurred by actors in the space environment due to the behavior, in terms of design and operational concept, of evaluated missions are tested to effectively quantify short-, near-, and long-term risks. This methodology is open and hence transparently available and compatible with present day space debris mitigation frameworks. The integral risk over all actors in orbit is the used environment capacity, i.e., the risk that we trigger a Kessler syndrome in the space environment. This value, including the predicted use by planned missions, can effectively be compared with space debris environment simulation models to identify sustainable trends. These trends can be tracked and accounted for on yearly basis. Where collision risk represents short-term physical interference with other actors, not tracking a sustainable trend represents the long-term physical interference with the environment.

In analogy with the *modus operandi* of the ITU, a space traffic management framework based on the philosophy of avoiding interference, based on the risk as defined in this work, would extend, rather than redesign, current national space debris mitigation frameworks into an internationally harmonized processes for space sustainability by ensuring space safety as the absence of harmful interference. Technological methods and processes to do so have been identified and prototyped. Adoption is pending.

## References

- Bastida Virgili B, Flohrer T, Krag H, Merz K, Lemmens S (2019) CREAM – ESA’s proposal for collision risk estimation and automated mitigation. In: 1st International orbital debris conference, Sugar Land, TX, USA, 9–12 December 2019
- European Space Agency (2019) ESA’s annual space environment report. GEN-DB-LOG-00271-OPS-GR Issue 3. [https://www.sdo.esoc.esa.int/environment\\_report/Space\\_Environment\\_Report\\_latest.pdf](https://www.sdo.esoc.esa.int/environment_report/Space_Environment_Report_latest.pdf)
- Inter-agency Space Debris Coordination Committee (2007) IADC space debris mitigation guidelines. IADC-02-01, Revision 1, September 2007. <https://iadc-home.org>
- Inter-agency Space Debris Coordination Committee (2017) IADC statement on large constellations of satellites in low earth orbit. IADC-15-03, Revision 0
- International Academy of Astronautics (2006) Cosmic study on space traffic management
- International Standards Organisation (2019) Space systems – space debris mitigation requirements. ISO 24113:2019
- International Telecommunication Union (2016) ITU radio regulations. <http://www.itu.int/pub/R-REG-RR/en>
- Kessler DJ, Cour-Palais BG (1978) Collision frequency of artificial satellites: the creation of a debris belt. *J Geophys Res Space Physics* 83(A6):2637–2646
- Krag H, Serrano M, Braun V, Kuchynka P, Catania M, Siminski J, Schimmerohn M (2017) A 1 cm space debris impact onto the sentinel-1a solar array. *Acta Astronaut* 137:434–443
- Krag H, Letizia F, Lemmens S (2018) Space traffic management through the control of the space environment’s capacity. In: Proceedings of the 5th European workshop on space debris modeling and remediation
- Letizia F, Colombo C, Lewis HG, Krag H (2016) Assessment of breakup severity on operational satellites. *Adv Space Res* 58:1255–1274
- Letizia F, Colombo C, Lewis HG, Krag H (2017) Extending the ECOB space debris index with fragmentation risk estimation. In: 7th European conference on space debris, Darmstadt
- Letizia F, Lemmens S, Virgili BB, Krag H (2019a) Application of a debris index for global evaluation of mitigation strategies. *Acta Astronaut* 161:348–362
- Letizia F, Lemmens S, Krag H (2019b) Environment capacity as an early mission design driver. In: Proceedings of the 70th international astronomical congress
- Maury T, Loubet P, Trisolini M, Gallice A, Sonnemann G, Colombo C (2019) Assessing the impact of space debris on orbital resource in life cycle assessment: a proposed method and case study. *Sci Total Environ* 667:780–791
- Rathnasabapathya M, Wood D, Jah M, Howard D, Christensen C, Schiller A, Letizia F, Krag H, Lemmens S, Khlystov N, Soshkin M (2019) Space sustainability rating: towards an assessment tool to assuring the long-term sustainability of the space environment. In: Proceedings of the 70rd international astronomical congress
- Rossi A, Valsecchi GB, Alessi EM (2015) The criticality of spacecraft index. *Adv Space Res* 56(3):449–460
- Tapio J, Soucek A (2019) National implementation of non-legally binding instruments: managing uncertainty in space law? *Air Space Law* 44(6):565–582
- The Consultative Committee for Space Data Systems (2013) Conjunction data message. CCSDS 508.0-B-1
- United Nations (1966) Treaty on principles governing the activities of states in the exploration and use of outer space, including the moon and other celestial bodies. RES 2222 (XXI). <https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introouterspacetreaty.html>
- United Nations (2019a) Guidelines for the long-term sustainability of outer space activities. A/AC.105/C.1/L.366
- United Nations (2019b) COMPENDIUM: space debris mitigation standards adopted by states and international organisations. <https://www.unoosa.org/oosa/en/ourwork/topics/space-debris/compendium.html>
- Utzmann J, Oswald M, Stabroth S, Voigt P, Retat I (2012) Ranking and characterization of heavy debris for active removal. In: Proceedings of the 63rd international astronomical congress



Xavier Pasco

## Contents

Introduction .....	866
Change of Strategic Landscape: A Succession of Disturbing Events .....	867
Early Armed Threats in Space .....	869
A Generic List of Possible (Intentional) Threats in Orbit: Assessing Offensive Realities of Today .....	871
What Vulnerability, in Which Context? Very Different “Defensive” Situations .....	874
The Notion of “Space Threats” and Its Relevance for the Security of Space Activities .....	874
Ground-Based ASAT Tests .....	875
Alleged Risks of “Cyberattacks” .....	875
The General Vulnerability of the Ground Segment .....	877
The Case of Orbital Hazardous Events: The Example of “Zombiesats” .....	878
The Jamming of Space Telecommunication from the Ground .....	879
Some Effects on Space Deterrence: Protecting Against What Threat and/or Vulnerability? ...	879
Conclusions .....	880
References .....	881

## Abstract

For roughly two decades, orbital systems, beyond their traditional strategic value, have gained a pivotal role in modern conventional security and defense activities. As a consequence, they have been considered as possible new targets in military confrontations, and the recent years have indeed demonstrated a renewed activity in the field of antisatellite researches and tests. This piece attempts to put these efforts in perspective and detail their different forms. It appears that besides the traditional kinetic destruction of satellites, leading to uncontrolled long-lived debris, other threats may have equally destructive consequences with more limited side effects. Directed energy weapons in orbit or even cyberattacks may

X. Pasco (✉)

Fondation pour la Recherche Stratégique (FRS), Paris, France

e-mail: [x.pasco@frstrategie.org](mailto:x.pasco@frstrategie.org)

become weapons of choice in the new space landscape. These likely perspectives must lead the international community to rethink the reality of threats related to space systems.

---

## Introduction

Space systems have gained an increasing importance in the everyday life of the modern societies: telecommunications by satellite, broadcasting of television programs, observation of the Earth's surface and oceans, observation of the atmosphere for weather forecasts, navigation, and worldwide broadcasting of universal time have so many applications that they contribute intimately to the day-to-day making of our contemporaneous world.

Besides, the needs for the defense of States and for the security and safety of their citizen feed widely on data resulting from the use of observation, electronic intelligence, or early warning satellites. These have contributed in an essential way to producing a strategic piece of information during these last 50 years, helping in the prevention of the bipolar crises. Chastely qualified as "national technical means," observation, electronic intelligence, or early warning satellites became one of the touchstones of the strategic dialogue of the 1970s and 1980s. In this context, keeping space safe and preventing any evolution leading to putting space systems in jeopardy became a key word. In particular, American presidencies of the Cold War had effectively resigned themselves to this established fact. For decades, according to recently published official US documents, it was clearly recognized that any preparation of an antisatellite interception would have been contrary to the spirit if not the letter of the SALT (Strategic Armements Limitation Talks treaty signed in 1972 by Richard Nixon and Leonid Brezhnev) protection of "national technical means" with the risky perspective "to stimulate satellite interception since we are more dependent on intelligence from space sources and would have more to lose." (Memorandum from the President's Assistant for National Security Affairs (Scowcroft) to President Ford, Washington, July 24, 1976. For a more complete vision of the position of the US authorities at that time, refer more largely to the archives recently published under the direction of McAllister (2009).) In spite of two Soviet campaigns of antisatellite attempts during the 1970s which led to the US executive authorities to reexamine this position and realize a first antisatellite test in 1985, this particular form of militarization of the space was hardly pushed, the possible earnings remaining considered very thin with regard to the incurred strategic risks. The "stabilizing" function of these national technical means during the Cold War had been already well established and has been well informed since.

Considering this central aspect, the club of the space countries quickly agreed on the interest of keeping space free of weapons, in an explicit way or more implicitly. The text of the main legal body, the "treaty on principles governing the activities of States in the exploration and use of the outer space, including the Moon and the other celestial bodies," came into effect in 1967, has established the idea according to which the exploration and the use of the space are the privilege of the whole humanity. It has dedicated the freedom of research and circulation in space and

has clearly indicated that the notion of State sovereignty cannot be extended in outer space or in the celestial bodies. Establishing the founding principle of the “peaceful uses” of outer space, the text does outlaw the deployment of weapons of mass destruction in outer space as well as any military activity on the Moon and on the other celestial bodies. (By the end of 2011, 100 countries had already ratified the Treaty, among which any major space nation.)

Nevertheless since approximately two decades, the international debate on the theme of the security of the spatial activities and more exactly on the militarization of the space returned to the front scene by becoming more radical. In the course of the transformations occurred during the 1990s, the initial preventions against a too extensive militarization of the Low Earth Orbit (LEO) have unmistakably weakened. Two main explanations can be called:

- The relative “downgrading” of the nuclear order as an international regulating principle and the consecutive “unbolting” of the debate on an increasing supposed vulnerability of the national spatial means: The United States in particular has mentioned the perception of an increased vulnerability considering the more and more central role played by satellites in the political, military, and economic life of most of the developed countries, with the United States in the first place.
- The emergence of new space actors, who may “threaten” to radically change the way space has been regulated under the auspices of a “club” of a few spacefaring countries, driving precisely these countries to anticipate this situation and bend over the elaboration of new international rules for the use of the space.

---

## **Change of Strategic Landscape: A Succession of Disturbing Events**

More than in the 50 last years, this decade has known several events that have underlined the fundamental fragility of satellites. A series of destructions in orbit, deliberate or not, put space in full light, worrying the largest part of the diplomatic and military community. It came in a way to punctuate harder and harder debates in Geneva on the prevention of the arms race in space.

1. First of all, the shooting by China of a ballistic missile towards an old weather satellite on January 11, 2007, leading to its destruction and to the generation of a 3000 long-lived fragments on a very busy orbit, surprised the whole world. This test was the first of its kind since the one undertaken in 1985 by the United States which proceeded to the interception of one of their satellite by using a missile embarked under an F-15 fighter plane.

At the very moment of the 2007 interception, the Chinese representatives were supporting without reserve the international efforts in the United Nations intended to limit the creation of space debris and opposed against the United States within the conference on disarmament in Geneva on the theme of the militarization of the space with a very proactive posture about prohibiting anti-satellite weapons.

2. Although they denied having had such intentions, the United States did not delay “answering” their Chinese counterparts by proceeding themselves on February 21, 2008, to the destruction of one of their military satellites in perdition. According to the American authorities, the point was to destroy a satellite which reentry was considered dangerous. Nevertheless, the successful attempt demonstrated, at least incidentally, the efficiency of one of the components focusing for the antimissile defense, whereas that it also meant the American intention “to mark” clearly its strategic territory. To complete the “state communication” picture, the American authorities did not miss to let know that this interception occurred at a much lower orbit than the Chinese interception, showing that this had been managed on the side of the United States in a more “appropriate way” by generating very short-term fragments of life. (Official US information has stated the figure of 175 detected debris (at the difference of 3037 for the Chinese event) with the last one reentered in the atmosphere by the end of October 2009.)
3. Less than a year later, on February 10, 2009, two satellites, one Russian (Cosmos 2251) and another one registered in the United States (a satellite of the Iridium constellation), collided and destroyed each other, generating some 1800 fragments on equally very frequented orbits. This collision, the first one in the history of space activity, was going to finish putting the question of space safety and security in the broad sense as one of the priority themes of the future space cooperation.
4. Finally, India performed an antisatellite test on March 27, 2019, using a two-stage ground based missile equipped with a terminal kill-stage that impacted a 750 kg Microsat-R satellite launched only about 2 months earlier in January 2019. This event was hailed by Prime Minister Modi as bringing “utmost pride” and having “a historic impact on generations to come.” Communication was visibly prepared to avoid the level of criticism brought about in its time by the Chinese test. In particular, a FAQ document published by the Indian MoD immediately after the test underscored that “the test was done in the lower atmosphere to ensure that there is no space debris. Whatever debris that is generated will decay and fall back onto the earth within weeks.” (See <https://www.mea.gov.in/press-releases.htm?dtl/31179/Frequently+Asked+Questions+on+Mission+Shakti+Indias+Anti+Satellite+Missile+test+conducted+on+27+March+2019> – accessed 29 March 2019.) Indeed, Microsat-R, supposedly an imaging satellite, was orbiting at about 280 km making it a “cleaner” target than the Chinese satellite, with debris supposed to burn in the atmosphere after only several months. It remains that this event has triggered the criticism of several operators of small low altitude satellites, such as Planet or Astroscale. However, it must be noted that the general reaction of governments, including China, has been limited to date.

Besides these well-known events, other recent disruptions in space have dramatized the space scene further, whether due to presumed cyberattacks (suspected in 1998 in the case of the US-UK-German satellite ROSAT recently reentered in the atmosphere), to laser blinding or tagging (as suspected from Chinese origin towards

an US NRO satellite in October 2006), to interferences, whether purposeful as in the recent case of an Eutelsat satellite jammed from a source in the Middle East or accidental with the so-called zombiesat belonging to Intelsat and uncontrolled between April 2010 and January 2011 while emitting at full power and interfering during this period of time with a number of telecommunication satellites. As it will be explained below, these latest cases must also be considered as potential major sources of disturbances.

---

## Early Armed Threats in Space

For a few years, the news has been dominated by controversies nourished by the supposed plans in a few countries of a possible deployment of weapons in the outer space. Such a subject is not new and has in fact been considered since the launch of the space activities. While no genuine “space arm race” has indeed been triggered during the Cold War, it is useful to remind nascent achievements in the 1960s, mainly carried out by the then USSR.

It must be noted that the “*weaponization*” of space has been considered very early in the history of space bipolar relationships. As early as February 1957, eminent US military officers did not hesitate to present space as a new “theater of operations”: “*In the long haul, our safety as a nation may depend upon our achieving ‘space superiority.’ Several decades from now, the important battles may not be sea battles or air battles, but space battles, and we should be spending a certain fraction of our national resources to ensure that we do not lag in obtaining space supremacy.*” (See excerpts of the famous 1957 speech by B. Schriever at <http://www.af.mil/news/story.asp?id=123040817> (accessed August 2012).) A few weeks after Sputnik, that same year, the Air Force Chief of Staff, General Thomas D. White, reiterated this general assessment, ensuring that “*whoever has the capability to control space will likewise possess the capability to exert control of the surface of earth.*” (Quoted in Stares (1985, p. 48). Military strategies would be also made public, for example, in a 338-page book, *The United States Air Force Report on the Ballistic Missiles* written by Colonel Kenneth Gantz (and forwarded by the well-known Generals White and Schriever). It was published by Doubleday and Comp in 1958. Besides the most common proposals aiming at developing antisatellite weapons, the US Air Force was proposing as soon as 1956 two different strategies for the military investment of space. One of those consisted in using a manned ballistic rocket (*Manned Ballistic Rocket Research System project*), while the other one (*Manned Glide Rocket Research System*) proposed the use of a reusable glide body launched from a main carrying rocket. If this latest project may recall the early NASA studies made about the shuttle at the end of the 1960s, this last project was purely military by essence as it envisioned the possibility to bomb the Earth surface since the altitude of 64 km! On its side, the Army, via the Army Ballistic Missile Agency (where Wernher Von Braun would ultimately help the United States to launch their first working satellite in January 1958), had the project of a super powerful rocket that would allow



“colonizing” the Moon as well as other planets for military purposes. For a detailed expose of the military position at that time, see also Baker (1985, pp. 12–30)).

If many projects aiming at militarizing space *stricto sensu* have emerged in the United States, none of them were given real credits by the successive presidencies in this country. The political authorities were more inclined to capitalize on the nascent nuclear ballistic force to ensure the strategic balance with the USSR. However, first initial developments made in relation with the ballistic threat can be cited that paved the way for ground-based space weapons. A first “missile defense” capability was proposed in 1958 with the two-stage Nike-Ajax nuclear armed antiballistic missile, later on followed by the more powerful Nike-Hercules and Nike-Zeus. First ABM interceptions occurred in 1962, opening the way to newer ABM missiles, namely, the Sprint and Spartan version leading to the “Sentinel” and “Safeguard” program in 1969 with the objective to defend a limited number of strategic missile silos. It must be noted that as early as May 1962, the then Secretary of Defense McNamara allowed the conversion of the Nike-Zeus model into an ASAT program (Program 505) which led to simulated interceptions and then to a successful hit in May 1963 against a cooperative target. Another existing ASAT capability based on the THOR missile was also operational and led to the shutdown of the Nike-Zeus capability. The THOR capability would also be terminated a few years later in the mid-1970s.

The USSR gave itself the first role in developing threats actually *coming* from space orbital systems. A first series of “co-orbital” tests were indeed carried out starting from 1968 with a first alleged success in November that year and ended in 1971, obviously at a time when the new “*Detente*” was to be consolidated after the US-Soviet signature of Salt-1. (Signed in 1972 in Moscow, this test was incidentally pleading for the use of National Technical Means for treaty verification.) Realizing an alleged total of five successful interceptions during the first series of seven tests, the technique used by the USSR was the “co-orbital” explosion carried out by a specifically designed orbital system within a kilometer-wide radius of the target. A second series of similar tests was undertaken between 1976 and 1982, based on the advocated need for the USSR to respond to future presumed ASAT capabilities expected from the US space shuttle then in construction.

The Soviet activity in the field was then perceived as highly intensive, and President Ford directed the start of an equivalent ASAT program that would ultimately take the form of an airborne missile launched from an F-15 *Eagle* airplane. After a few test launches performed in 1982 and 1985, a third launch ended up with the interception of a US satellite target directly hit by the so-called Miniature Homing Vehicle (MHV), the third stage of the ASM-135 Vought missile. Again, the program was officially phased out in 1988, in a context when the strategic and budgetary soundness of such projects was questioned.

In any case, this early history amply demonstrates that initial ASAT programs had been envisioned as being possibly part of the global arsenals from a military perspective if not from a political one. Only the key role played by spy satellites in the mutual nuclear deterrence prevented weapons in space from becoming operational during the Cold War. This did not prevent national R&D projects to develop, paving the way for possible future threats in space.

## **A Generic List of Possible (Intentional) Threats in Orbit: Assessing Offensive Realities of Today**

In today's completely renewed strategic context, these early antisatellite efforts have regained some momentum. Early programs have clearly served as a basis for more sophisticated projects allowed by technical advances, while new research domains seem to have emerged. The analysis of over more than two decades of R&D efforts lead to the following list of existing R&D orientations, possibly leading to actual space weapons:

- *Kinetic energy weapons* (KEW) implying a physical effect on the target, either by direct impact (so-called "hit-to-kill" techniques) or nearby explosion creating killing debris (such as in the case of the co-orbital Soviet systems)
- *High-altitude nuclear weapons* (EMP) creating ionization and/or electromagnetic effects on objects in the affected zone
- *Directed energy weapons* (DEW) mainly using laser or microwave techniques depositing energy on the target

Obviously other kinds of threats on space systems exist such as electronic warfare weapons (EW) using jamming techniques rendering communications impossible, or cyberattacks. Exactly like in the case of ground-based interceptors, such threats do not necessitate the use of space platforms to be effective. For this reason, such threats have not been treated as a key issue in the context of this chapter, as they do not define per se a threatening "space system." However, they shall not be discarded as their reality is largely tangible today as it will be explained further below.

- *Kinetic energy weapons*, while simple in their principle (physical collision), do not use simple techniques. They imply the use of maneuvering satellites as well as the mastering of precise "*rendezvous*" techniques, the least to achieve in case of "*hit-to-kill*" weapons! This can be related to techniques implemented by a number of existing systems, going from experimental surveillance satellites (or so-called "inspector" satellites) used, for example, to picture other orbital systems (such as in the case of the US XSS 11 and 12 or the Chinese SJ-12 or SJ-06F systems), to the European *automated transfer vehicle* (ATV) used for service and precise docking with the International Space Station (ISS). All these systems have in common highly maneuvering capabilities as well as precise terminal guidance systems allowing effective orbital "*rendezvous*." Mastering such technologies would theoretically allow developing kinetic energy ASAT. Protecting any satellite against the kinetic effect at orbital speeds becomes virtually impossible with pellets more than a few centimeters in size. As a matter of fact, protecting any satellite against a kinetic threat is almost paradoxical in itself. Satellite architectures are indeed based on the use of as light materials as possible involving some level of fragility. This is the case for satellite buses or for on-board solar arrays. "Armored" space systems are then hardly feasible and in any case would increase

cost at all levels, from development to launch. Only some level of physical protection against small-sized debris (in the millimeters scale) can reasonably be applied nowadays.

However, if they can represent deadly threats, KE techniques remain highly costly in terms of energy (most notably when changes of orbits would be needed for performing an intercept) and, in a more sensitive manner, would create more debris that would add to the already rather congested orbital traffic. For sure, creating more debris would not account among the most preferred offensive strategies for most of the spacefaring countries whose space systems rely on an undisturbed and clean orbital space. Nations that do not intensively use space might possibly be less deterred from such actions.

- *High-altitude nuclear explosions* would make use of a nuclear bomb sent at an altitude of a few hundreds of kilometers with the objective to create highly intensive electromagnetic disturbances for Low Earth Orbiting (LEO) and even geostationary (GEO) objects. Cold War years were soon followed by the fear of an increasing nuclear proliferation that would make such a possibility more probable. Such an attack could indeed have an enormous effect on the whole activity in space, with, in the first place, the possibility for the attacker of annihilating a number of military systems precisely destined to warn against nuclear attacks, such as early warning systems, Earth observing, signal interception, or strategic communication satellites. In such a situation, most of the non-protected space systems would also be destroyed.

Major studies (such as the HALEOS study published in 2001 under the auspices of the U.S. DoD Defense Threat Reduction Agency - DTRA) have shown that, compared with a terrestrial explosion, electromagnetic effects of a nuclear charge in space might be increased leading to potentially devastating impact beyond the only targeted orbits with short-term effects on the propagation of radio and radar waves, and longer-term effects involving the permanent excitation of Van Allen belts, with even the possibility of creating new magnetic belts resulting from the sudden expulsion of charged particles.

While ionizing effects would be specific to such explosions, other effects, such as electromagnetic effects, would be no different from those created by *directed energy weapons* (DEW) using high-power microwaves (see below). As a consequence, protecting any system against such threats would mean protecting it partially from a major consequence of a high-altitude nuclear detonation. In other terms, the main characteristic of such a nuclear threat would remain its “nondiscriminatory” effects on the whole orbital population. In any instance, such an attack would mean that a situation of war would preexist. This makes the use of nuclear attack clearly different from other intentional actions that might take place in more ambiguous scenarios or even in a covert manner.

- *Directed energy weapons* (DEW) are sometimes perceived as presenting a coming threat for space systems. Indeed, this threat is theoretically characterized by some level of intensity leading to likely modulated effects on the target. It can be

considered that DEW may have basically three classes of effects ranging as follows:

- Level 1: *A jamming effect*, i.e., time-limited disturbance of the satellite functioning that ceases when exposure to the weapon is over
- Level 2: *A disruption effect*, i.e., permanent disturbance (without definitive destruction) requiring an external intervention or reset
- Level 3: *An annihilation/destruction effect*, i.e., definitive disruption requiring an external replacement or repair at best. (This subjective scale can be paralleled to what has been almost theorized, or at least symbolized, in some US Air Force doctrinal documents using the infamous “5 Ds” to materialize the scale of gravity of any space attack: “*D* eception, *D* isruption, *D* enial, *D* egradation, *D* estruction.” See USAF (2004), Counterspace Operations, Air Force Doctrine Document, 2-2.1.)

DEWs may have different effects according to their domain of functioning: For example, an intense laser ray has a thermomechanical effect on any material and as such can neutralize or destroy sensors or even some structures. By contrast, a microwave weapon would not have any thermal effect but would produce instead a high-power electrical effect on electrical components, whether directly or indirectly. Low-level components such as receivers or some class of sensors would prove particularly vulnerable to such threats. As envisioned by largely publicized projects very early on (such as the US Space-Based Laser project), equipping space platforms with powerful lasers for ASAT kind of activities might be theoretically possible with the objective to overflow or even destroy targeted sensors. However, aiming at sensors might not be an easy task, with the additional possibility of the development of self-protection devices for the most sensitive satellites.

The literature has frequently referred to powerful lasers in orbit, mainly inherited from the early R&D experiments engaged during the Ronald Reagan years under the auspices of the United States, so-called Strategic Defense Initiative (SDI) often dubbed “*Starwars*.” (In this respect, it must be reminded that, at its apex, one of the several versions of this project was envisioning the deployment of many space and ground-based laser systems, possibly relayed by orbiting mirrors in order to destroy reentry nuclear heads. This complex network of sensors and effectors was considered as an addition to some more conventional 4000 intercepting “hit-to-kill” missiles or even satellites.) Laser-based ASAT developed under such concepts would be much more powerful with the objective to bring about mechanical destructions on the structure itself of space systems, most notably on deployed solar panels. Obviously, the development of such an armament would require much more energy generation that would make their development very problematic given the usual constraints applied to any space systems (size, weight, reliability). It is highly probable that these many technical constraints have largely put into question the development of such systems, even if it is probable that more or less secretive R&D has not ceased in this area. Following this logic, powerful microwave systems may represent a more threatening technology from an operational point of view than space-based lasers.

---

## **What Vulnerability, in Which Context? Very Different “Defensive” Situations**

Of course, any offensive weapon will focus at the main vulnerabilities of spacecrafts. These vulnerabilities are usually related to support functions such as:

- Attitude control
- Tracking and telemetry
- Thermal management
- Power management

The dysfunctioning of any of these technical functions would generally mean a shutdown of the entire system in short or longer term. As a result, the attack modes may be very diverse, whether they involve the destruction of the solar arrays, the thermal increase of the satellite structure, or a cyber intrusion in automated management processes.

In addition, the vulnerability of any spacecraft can vary quite largely considering their very nature, the applied management processes, and even the very mission it has to fulfill. As an example, telecommunication satellites are controlled by multiple operators, private or public, which sell their services to many customers. In this particular case, many motivations can exist for attacking the space system, from a hostile action against a specific customer to a more “wide-range” terrorist-like attack. This means that the ways and means used for attacking the “satcom” function can be very different from an action to another, implying the need to protect many dimensions of a complex system. (Obviously, the uplink remains the targets of choice for any action against the satellite itself.)

As for the navigation satellite, their systemic redundancy makes them less an easy target. In this case, jamming may be used but this time with local effects, as it has been sometimes the case during the recent conflicts using GPS-guided munitions. In the case of Earth observation satellites, in addition to their highly critical pointing and control systems, their sensing payload and their downlink communication systems appear as high-value potential breaches. This vulnerability is indeed increased by their relatively few numbers and by the accessibility of the Low Earth Orbit (LEO) they usually make use of. Last but not least of this non-exhaustive list, the weather satellites, while mainly on the geostationary orbit, may also be vulnerable due to the reliance on the good functioning of their sensors as well as on their communication downlink capacity. It is obviously reinforced for those satellites that orbit on LEOs.

---

## **The Notion of “Space Threats” and Its Relevance for the Security of Space Activities**

As just shown above, the notion of “space threats” as strictly defined by space systems posing a threat in orbit might not reveal itself as the most urging issue to tackle. Indeed, most of the space systems that might be considered as potential offensive candidates seem to remain fairly confined to the prospective horizon. From

a technical standpoint first, using space systems as offensive weapons is not a simple operation. It involves relying on very demanding systems (in terms of sensing, maneuverability, energy management, cost, etc.) that may not make them so easy to produce and use. From an operational point of view also, this complexity may not be what a military user is looking for, notwithstanding the fact that, in the case of using offensive KEWs, the consequences of any attack will make no discrimination in the end between the victim and the attacker. For this reason, and from the policy perspective, it seems reasonable to put into question the very relevance of “threats in space” as a central notion for building the core of the future of space security. For sure, such a view does not imply that the international community should not pay attention to these developments. On the contrary, the fact that such techniques might be used one day should trigger a widespread awareness that in this field, earliest actions against the development of such weapons will be the most efficient. But in parallel, the rather prospective nature of these kinds of threats must not lead space-leading countries to underestimate the importance of other sorts of threats that may be much more meaningful on the shorter term. A brief (non-exhaustive) list of such threats may be recalled.

### **Ground-Based ASAT Tests**

The most recent ASAT tests performed in 2007, 2008, and 2019, respectively, by China, by the United States, and most recently by India provide a good example of the practicability of and efficiency of ground-based ASAT missiles. As mentioned at the beginning of this chapter, the first one performed by China in January 2007 destroyed a decommissioned Chinese weather satellite on an 800 km circular orbit. A little bit more than 1 year later, the United States did hit a lower orbiting military satellite (246 km) with the stated goal to prevent an uncontrolled and dangerous reentry. In the first case, the interceptor used was a modified SC-19 missile, while the US military used the SM-3 sea-based intercepting missile developed for ABM purposes. Obviously, the proximity of anti-ballistic missile research and ASAT interceptors has been clearly apparent in all cases. While not completely known to date, the interceptor used by India has been officially acknowledged as a “DRDO’s Ballistic Missile Defence interceptor (...) which is part of the ongoing ballistic missile defence programme” (Idem). It must also be recalled that China did several allegedly ABM high-altitude related tests in the aftermath of the 2007 ASAT experiment.

Even if it must be recalled that the targets were mainly cooperative and their trajectory well is known from their “attackers,” these three cases have however amply demonstrated how much mastering space interception from the ground has become accessible to the most prominent ballistic and space powers.

### **Alleged Risks of “Cyberattacks”**

Another type of risks, the “cyberattacks,” has been alleged as becoming a major cause of concern for space systems. Cyberattacks can indeed take many forms and

affect many elements of the entire space and control system. Tracking, telemetry, and control networks can be subject to such cyber-threat with the impossibility to transmit reliable data for the control of the satellite platform. As a consequence, any satellite can virtually be taken over by a non-authorized user who can force a system shutdown or a wrong maneuver leading the system to put itself in a safe mode or in any other uncontrolled mode. In theory, such a takeover can be implemented via cyber intrusions in the command center or through key ground stations. Awareness about the possibility of such attacks has increased over the recent years. In 2001, a NASA audit report pointed out that “six computers servers associated with IT assets that control spacecraft and contain critical data had vulnerabilities that would allow a remote attacker to take control of or render them unavailable.” (The report goes on blaming that “moreover, once inside the Agency-wide mission network, the attacker could use the compromised computers to exploit other weaknesses we identified, a situation that could severely degrade or cripple NASA’s operations.” Source: NASA (2011).) These conclusions have been largely commented and have motivated the adoption of unprecedented protection measures for the Agency space systems.

A few recent cases have sometimes been cited that seem to sustain this assessment:

- Some reports have claimed that the German X-ray satellite ROSAT (made famous recently due to its uncontrolled reentry during the night of October 22–23, 2011) had been targeted in September 1998 by a cyberattack leading it to wrongly orient towards the Sun, ultimately causing its shutdown. This “wrong maneuver” (the cause of a loss of the satellite sensors) is reportedly related to a cyberattack carried out against computers of the Goddard NASA Center as unveiled in 1999 by one of the specialists in charge of the center computer services. At this time, the attack perpetrated against the X-ray department of the center was attributed to a Russian origin. However, those facts have never been confirmed, just a “troubling” coincidence between the move of the satellite and an intrusion in the computer system having been officially mentioned by the inquiry.  
Another satellite, INSAT-4B-S, this time a telecommunication satellite belonging to India has been mentioned as having been affected by a cyberattack (*Stuxnet Worm*) that would have caused a severe loss of power, ultimately leading to reduction of the telecommunication capacity of the satellite by more than 50%. (Again, this case has not been fully acknowledged, yet some other hypothesis (supported by ISRO) points out the loss of one of the solar arrays of the spacecraft. No official position about the incident has been confirmed up to this day.)
- Other examples have been cited in draft U.S. Congress reports citing interferences having affected the Earth imaging Landsat-7 satellite at least twice in 2007 and 2008, while another NASA EO satellite, TerraAM-1, experienced the same disruptions in 2008, for more than a single day in one occurrence. More recently, the U.S. National Oceanographic and Atmospheric Administration (NOAA) is reported having suffered a disruption of its Satellite Data Information System due to a severe hacking incident in September 2014. This implied for the Agency being denied sending weather forecast data for 48 h. (These episodes are

mentioned in Lewis (Patricia), Livingstone (David), “Space, the Final Frontier for Security,” Research Paper, Chatham House, September 2016, p. 10. See also 2011 Report to Congress of the U.S.-China Economic and Security Review Commission, pp. 215–217 ([https://www.uscc.gov/sites/default/files/annual\\_reports/annual\\_report\\_full\\_11.pdf](https://www.uscc.gov/sites/default/files/annual_reports/annual_report_full_11.pdf).) Some other attacks occurred on NOAA satellite in October the same year, with press reports about Chinese hacking attempts. (See “Chinese Hack U.S. weather system- satellite network,” Washington Post, 12 November 2014.)

Of course, another more generic risk is represented by a cyber intrusion in the information chain itself (data collection, processing, and dissemination) without affecting the satellite itself. This type of attack, even if indirect, may have consequences as serious as if the space segment itself was the target, for example, ending up with wrong data, unreliable imagery, and false alarms. While targeting only information, this type of intrusion can barely be deterred by strictly “space segment-oriented” defensive strategies and doctrines.

Cyberattacks will probably account for the most preferred offensive strategies when the objective will be to disrupt an entire “space system,” especially when they are old generation, i.e., not protected against the latest software offensive devices. Here again, the capability to detect the origin of the attack and to attribute its responsibility will be the key for an effective deterrence strategy. At this level, there is no magic for space systems, and this type of vulnerability is essentially linked to a domain that remains partly external to the space sector itself.

## **The General Vulnerability of the Ground Segment**

More generally, the ground segment represents a key node for ensuring the functioning of any space system. Losing the ground segment necessarily means losing the space segment. In theory, the consequences on the long term might be less definitive than when a spacecraft is destroyed, as regaining control on the operation of the space system might be possible once the functions of the ground segment have been recovered. Hence, losing the control of the ground segment might be considered as a reversible situation and might not imply the same kind of strictly deterring positions as in the case of the space segment.

However, the border between both situations may sometimes be very thin, as taught by a case occurred to Russian satellites more than 10 years ago, in May 2001. As reported at that time, a fire destroyed almost completely a main control station leading to a total loss of communication with four military early warning satellites placed on a highly elliptical orbit Podvig (2002). Only one satellite has been recovered after a while, the three others having derived well beyond their nominal position. Those remained well out of reach by their dedicated ground segment. This “ground” damage has then become irreversible for the space segment itself. It may even include risks for other spacecraft, proving at this occasion that the safety management of satellites may be key in collective space security.



Here again, protecting the ground segment against attacks or hostile actions does not directly imply the protection of the space segment only. It may involve some level of “systemic” thinking, some redundancies (ground and space), as well as some parallel hardening techniques (e.g., against high-power microwave devices or even to prevent possible EMP effects). In addition, the adoption of degraded modes must also be considered for any key node on the ground. It is important to note that such measures must apply to both military and civilian satellite owners to be fully efficient.

## **The Case of Orbital Hazardous Events: The Example of “Zombiesats”**

*A contrario*, from April 2010 to January 2011, Intelsat, the largest telecommunication satellite operator, has lost control over Galaxy 15, one of about sixty satellites composing its geostationary fleet. This spacecraft has derived over a large portion of the geostationary orbit without offering any possibility for being recovered during that 8 month long time. This event has had a double consequence:

- An increased collision risk affecting the whole community of the satcom users, civilian, and military.
- A powerful jamming of satellite telecommunications as Galaxy 15 has kept on emitting at full power during the whole period of time. One of the most documented consequences was the loss of WAAS (the US regional GPS *Wide Area Augmented System* for improved satellite navigation) in Alaska.

The control of this satellite (quickly nicknamed “zombiesat” in the large amount of literature devoted to this case) has finally been recovered in January 2011 by Intelsat. However, this case has amply shown what kind of disturbances such an event can create with the necessity for operators to avoid possible collisions and interferences. (For example, it has been reported that, at this occasion, SES, the second largest geostationary satellite operator, had to proceed with many very precise maneuvers around some of its strategic orbital positions.) It shows how much non-intentional actions can also present serious threats to space security that do not clearly relate to deliberate actions. There may be a specific vulnerability in face of such “zombiesats” on the geostationary orbit due to the vicinity of the satellites around some key orbital positions. This must be taken into account as a complexity factor of the collective space security, as this makes disturbances rather quick to produce, intentionally or not, both for civilian and for military systems. It must be noticed that operators have seized the importance of such potential developments and have chose to share their knowledge by setting up a common database allowing them fostering early and precise coordination when needed. (Via the creation in 2009 of the Space Data Association, based on the Isle of Man. Obviously, considering the wealth of information contained in those databases, such a private initiative cannot be without consequences on the general management of international relations in space.)

## The Jamming of Space Telecommunication from the Ground

Of course, last but not least, the simple jamming of space telecommunications by using ground-based devices must also be evoked in this list of “indirect” space threats. One of the most recent Iranian episodes (spring 2009) can be quoted as the Iranian government has decided to jam two satellites (*Hotbird 6/8 W6*, *Eurobird 9A/2*) managed by Eutelsat, one of the two major European telecommunication operators. The goal was then to prevent the broadcast of information perceived as contrary to the Iranian regime interest. The cost to access such technologies is relatively low at the level of a government, and these interferences remains sometimes hard to detect when they occur and in any case highly difficult to prevent. A contrario, the example quoted here, has shown that, for a time, operators themselves had been dissuaded to broadcast the controversial information (BBC and VoA notably).

All these examples show clearly that direct threats on space systems, as evoked in the first part of this chapter, do not represent the sole source of possible security breaches. They may not even appear as the most probable cause of space insecurity, at least for the short to middle term. The difficulty remains both the attribution of responsibilities and, more difficult even, the establishing of the intentional nature of any catastrophic event. Any questioning about the setting up of international regulation, whatever their form, or of some sort of “space deterrence” must take this complexity into account.

---

### Some Effects on Space Deterrence: Protecting Against What Threat and/or Vulnerability?

In light of these possible developments, thinking about future threats on space systems means thinking about the probable nature of those treats as well as the kind of possible enemy using them. At first glance, the most developed spacefaring nations have used their space assets in a strongly asymmetrical context in which only a few countries were able to use similar orbital systems, possibly in a hostile way. However, it is probably necessary to take into account other kind of threats that countries on the verge of becoming space powers might likely use in case of political or military showdown.

Generally, deterring any threat to develop against space assets will imply a large appreciation of this diverse nature of possible threats, whether intentional or non-intentional. This approach will probably go through a few preliminary protective postures and actions:

- **Establishing the capability to attribute an effect to a certain cause:** This capability, addressing either intentional or non-intentional threats, relies on very specific technical capacities whether they aim at monitoring LEO or GEO orbits. But, in parallel, according to the nature of the threat in orbit (KEW, DEW, Jamming, etc.) or from the ground (using the same kind of techniques in a different way), very different means will have to be implemented to protect the

satellites. Some strategies may envision having on-board devices allowing detection (and characterization) of laser attacks, for example. This may bring about a certain deterrent effect against an adversary who would rather have acted stealthily. Some other will possibly envision satellites more directly dedicated to detection and inspection. Of course, ultimately, these “defensive” systems may appear in reverse as potentially challenging this quest for permanent capacity to attribute any event to a certain cause. Indeed, by definition, such protective devices would make use of technologies that may allow discreet and more offensive actions. This is not the least of the paradoxes that such efforts would imply.

- **Creating a “red line” against any attack:** Provided the cause of any event solidly established, the difficulty remains to establish a sort of “red line” beyond which military protective action would be legitimate. First, characterizing between the intentional or the non-intentional move will be key in determining the reaction of the “victim.” There probably lays the most difficult issue to tackle when it comes to ensuring a comprehensive protective posture (including military) against any threat on space systems. It must be noted that even in the case of a recognized intentional action, the possible “graduate” nature of the hostile action (from deception to *destruction* to recall the “5 Ds” approach) may render difficult any decision about the nature of the counteraction itself. This aspect may be at the center of the current effort to establish “rules of the road.” No doubt that it will also raise expectations about the resistance capacity of the next-generation space assets. This is the approach followed for the hardening of the electrical components, for example, with two (possibly contradictory) principles. Making well known that the considered system has been hardened while, at the same time, keeping any possible adversary in the impossibility to determine the methods and the techniques used, as well as the very level of this hardening.

---

## Conclusions

In any event, the road towards limiting by principle threats on space systems in a significant manner will probably remain quite bumpy for a while.

At this stage, satellites have remained vested with a highly symbolic value that continues to put them at the center of the current strategic relationships. The latest events (comprising the March 2019 Indian ASAT test as well as the Chinese ASAT in 2007 and in a way the US-made satellite destruction in 2008) have shown that affirming this kind of capability was also a part of “deterrence” postures or “state communication policies.” It is well documented that satellites will become smaller and smaller, more and more able while less and less costly. The generalization of smaller high-performance spacecraft (whether military or civilian), possibly “launched on demand,” announces the beginning of a new era for which a new equilibrium will have to be found. These progresses, sometimes promoted through concerted national efforts, are also a part and parcel of the “equation” aiming at balancing the protective approach with bolder technology-led solutions that are

supposed to give an edge to the more advanced space countries. (Such as in the case of the US *Operationally Responsive Space* program, for example, even if this effort seems to remain in question nowadays.) Answering this question and finding a workable balance will determine the fate of our collective security against the threats on space systems as well as it will orient the future nature of a possible “space deterrence.”

---

## References

- Baker D (1985) The history of manned spaceflight. New Cavendish Books, London
- Caldicott H, Eisendrath C (2007) War in heaven: the arms race in outer space. The New Press, New York/London
- Department of State (2009) Foreign relations of the United States, 1969–1976, vol E-3, documents on global issues, 1973–1976. United States Government Printing Office, Washington, DC
- Gantz K (1958) The United States air force report on the ballistic missiles. Doubleday & Comp, New York
- HALEOS, High-Altitude Nuclear Detonation against Low Earth Orbit Satellites (2001) Defense threat reduction agency briefing. <http://www.fas.org/spp/military/program/asat/haleos.pdf>. Accessed Aug 2012
- McAllister WB (2009) Foreign relations of the United States, 1969–1976, volume E-3, documents on global issues, 1973–1976. United States Government Printing Office, Washington, DC
- NASA (2011) Inadequate security practices expose key NASA network to cyber attack, office of audits, Washington, DC. For the complete audit document, see <http://oig.nasa.gov/audits/reports/FY11/IG-11-17.pdf>. Accessed 20 July 2012
- Podvig P (2002) History and current status of the Russian early warning system. *Sci Glob Secur* 10:10–60
- Schriever B (1957). <http://www.af.mil/news/story.asp?id=123040817>. Accessed Aug 2012
- Stares P (1985) The militarization of space, U.S. policy, 1945–1984. Cornell University Press, New York
- Stares P (1987) Space and national security. The Brookings Institution, Washington, DC
- USAF (2004) Counterspace Operations. Air Force Doctrine Document 2–2.1. [http://www.dtic.mil/doctrine/jel/service\\_pubs/afdd2\\_2\\_1.pdf](http://www.dtic.mil/doctrine/jel/service_pubs/afdd2_2_1.pdf). Accessed Jan 2010



# European Space Surveillance and Tracking Support Framework

# 46

Regina Peldszus and Pascal Faucher

## Contents

Introduction .....	884
Governance .....	885
Background .....	885
Legal Basis .....	887
A Consortium of European Member States in Cooperation with Council Agency .....	888
Internal Governance .....	889
Interaction with European Union Stakeholders .....	891
Transatlantic Relationship .....	891
Operations .....	892
Service Provision Model Based on Internal Specialization .....	892
Sensor Network .....	893
Data Processing & Data Policy .....	894
Services .....	895
Users .....	896
Perspectives .....	897
Evolution as a Sensor Network .....	897
Evolution in the EU Space Program .....	898
Evolution in the Context of Space Traffic Management .....	899
Conclusion .....	900
References .....	901

---

R. Peldszus (✉)

Department of Space Situational Awareness, German Aerospace Center (DLR) Space Administration, Bonn, Germany  
e-mail: [regina.peldszus@dlr.de](mailto:regina.peldszus@dlr.de)

P. Faucher

Defence and Security Office, French Space Agency (CNES), Paris, France  
e-mail: [pascal.faucher@cnes.fr](mailto:pascal.faucher@cnes.fr)

---

**Abstract**

In order to safeguard European space infrastructure and contribute to global burden-sharing in the domain of Space Situational Awareness, the European Union set up a dedicated capability for Space Surveillance and Tracking (EU SST). Operational since 2016, EU SST employs a novel governance model that joins existing sensors of European Member States and provides collision avoidance, reentry and fragmentation analysis services to the European user community. This chapter provides an overview on the formation, internal governance, and operations of the current European Space Surveillance and Tracking Support Framework and offers a perspective on its future as part of the proposed EU space program.

---

**Introduction**

The capability of Space Situational Awareness (SSA) – monitoring and understanding real-time and foreseeable developments of activity in the orbital environment – has become a fundamental prerequisite for space security, both as a means for transparency, information advantage, and verification and as operational foundation for the resilience of space-based systems. While the major space actors maintain SSA capabilities to varying degrees (Lal et al. 2018), the US Strategic Command currently operates the most sophisticated SSA capability with dedicated data exchange arrangements to external state and non-state actors (West 2018).

Yet, not only is the safeguarding of the near earth environment as a global commons an international concern in the advent of an unprecedented scale and variety of activities across orbital regimes. The necessity for significant investment into development and operation of SSA sensor systems also lends itself to collaborative rather than unilateral efforts (McCormick 2013). In Europe, despite a range of sensor systems, governmental and commercial actors have been relying predominantly on SSA data provided by the United States. However, it has become paramount for Europe, particularly institutional actors such as the European Union, to protect their own space-based infrastructure, such as the Galileo navigation system. Furthermore, reaching a greater level of autonomy in space surveillance through a dedicated capability allows Europe to contribute to global burden-sharing in the domain of SSA and to enhance its position in international discussions (Pellegrino and Stang 2016, pp. 47–48; Dickow 2015, p. 123).

Hence, in recognition of the need for non-dependence in detecting risks in orbit and the opportunity offered by existing SSA legacies and advanced sensor capabilities in Europe, the European Union has since 2014 undertaken concrete efforts to consolidate a SSA capability. Initial focus was placed on one of the key elements of SSA (cf. European nomenclature (Rovetto and Kelso 2016)), Space Surveillance and Tracking (SST): sensor systems, such as radars, telescopes, and lasers, deliver data on the location and behavior of active and non-active spacecraft or debris, based on which risks can be evaluated on objects that are at risk of collision, have fragmented, or will reenter the atmosphere. By incentivizing the networking of hitherto discrete sensor assets already operated by separate entities in Europe, the European Space

Surveillance and Tracking Support Framework (EU SST) today constitutes the EU's primary SSA capability.

This chapter provides an overview about context, implementation, and perspective of the European Union's Space Surveillance and Tracking Support Framework. Following an outline of the political developments leading up to its formation, an overview on the internal governance of EU SST and its organization as a cooperation of EU Member States and a council agency is provided. Subsequently, its three operational functions are described that network SST sensors process SST data and form the basis for SST services to a varied user community. The chapter concludes with a perspective on how EU SST is bound to develop as part of the upcoming space program of the European Union and how it slots into to the emerging technical discourse on future space traffic management and coordination regimes.

---

## Governance

### Background

The notion of devising and implementing a dedicated European SST capability emerged in the decade preceding the adoption of the legal basis in 2014. European actors – with impetus from the new space policy mandate of the Lisbon Treaty – became either more aware of pending space security challenges in general or had already begun specifically to tailor, develop, or analyze possible responses to the safety and security challenges in the space domain. Increased non-dependence from US capabilities and contribution to global burden-sharing was already a central consideration, including the necessary trade-off between sovereign requirements and a degree of collective autonomy.

In response to a changing security environment after the Cold War, the European Union had begun to assess emerging drivers for future crisis management and related space operational requirements. In the string of critical space-based services including Earth observation (EO) and position, navigation, and timing (PNT), a space surveillance system was highlighted as a fundamental capability gap and priority of a future European space program (Commission of the European Communities 2003; SPASEC 2005). This was understood both in the context of more independently meeting the needs of burgeoning space efforts in Europe but in turn also to contribute to global burden-sharing, particularly with regard to efforts of the United States (Conclusion of the Workshop on Security and Arms Control in Space and the Role of the EU, 2007, cited in ESA 2008, p. 6). A Space Council Resolution then underlined the need to fill the capability gap of SSA, in order to accommodate safeguarding of space-based assets and infrastructure (navigation and observation) on the one hand and enable non-compliance and treaty verification on the other (Council Resolution 2008).

In view of this, the need for cooperation across multiple actors – rather than unilateral efforts – including across the civil-military intersection had already been recognized as a necessary key characteristic of emerging SSA efforts of European state actors and supranational and intergovernmental bodies (Spasec 2005). Of the European Union Member States, only France, the United Kingdom, and Germany

had operational space surveillance capabilities at the time (Pagkratis 2011, p. 98; Veclani et al. 2014, p. 39 and 40), which were integrated or coordinated to some extent with European or transatlantic partners. A UK asset (Fylingdales) was part of the US Space Surveillance Network (US SSN). A bilateral Franco-German use of space surveillance and tracking radars (GRAVES and TIRA) had been underway since 2006 (Pasco 2009, p. 34; McCormick 2015, p. 46) and was explored as a potential model for the pooling of capabilities in a broader European framework (Robinson 2011, p. 21) or for possible approaches to data exchange or processing (European Commission 2013b, p. 13).

Meanwhile, the optional program for SSA at the European Space Agency (ESA) commenced work in 2009 (ESA 2008) borne out of earlier efforts in determining needs and requirements of a SSA system with a variety of stakeholders (Marta and Gasparini 2008, pp. 139–40) (Many of the participating countries were both ESA and EU Member States.). In this context, a range of studies explored possible approaches to a European SSA system: an architecture analysis examined three options of ground- and space-based SSA infrastructure, highlighting the merits of synergies of a comprehensive approach to including the monitoring of space objects and the space environment (Donath et al. 2009) (N.B. the different nomenclature of SSA in Europe to include SST, SWE, and NEO (the latter elements summarized as space environment in non-ESA contexts), in comparison to US nomenclature that included intelligence, surveillance, reconnaissance, environmental monitoring, and command and control (cf. Rovetto and Kelso 2016, p. 3)). Another comparative study on governance explored existing and potential models relating to organization and data policy, examining different models for decision-making including program-oriented and institution- or policy-oriented in the European Union (Pasco 2008). In trading off the constraints of national security interests with the potential of collective effort, it sketched the potential setup of a European supervisory authority overseeing the work of a managing organization, already accounted for different security requirements of the two central missions of space object surveillance (SST) and space environment monitoring (space weather and NEO).

At the same time, dialogue among the Member States of both EU and ESA was ongoing as to which body would be best suited to account for the political and practical security requirements of individual space actors involved in collective SSA efforts in Europe (Chow 2011, p. 11; Nardon 2007, p. 6). With the increasing involvement and consolidation of the European Union in space governance (Mazurelle et al. 2009, p. 18; Council Resolution 2010), additional EU bodies entered the debate. The EU's European Defence Agency (EDA) defined military user requirements (EDA 2010), which were later fused with civilian mission requirements in a dedicated set of high-level SSA civil-military use requirements (Council of the European Union 2011). Consultations between the EU and EU Member States' space agencies and ministries from 2009 onward had affirmed the emerging role of the EU as actor in space security matters and SSA in particular and were accompanied by further external studies on overall governance (European Commission 2013b, pp. 6–7).

As part of the continuing momentum for a European endeavor, a consensus emerged that an operational SST system be situated within the remit of an effort



established and managed by the EU (Veclani et al. 2014, p. 40 and 74; Space Security Index 2012, p. 49–50). The de facto shift of the constituent national actors towards a setting as part of the European Union was formalized as part of the Space Council Resolution of 2010. It subsequently entailed a divestment from operational SST elements of ESA's SSA program (McCormick 2015, p. 48; ESPI 2018, p. 54), which continued with renewed focus on research and development for SST and on space weather and near-Earth objects (Flohner and Krag 2017).

Interactions were also extended beyond Europe to inform and engage with regard to emerging governance options. Existing bilateral channels on SSA between EU Member States and their US counterparts (Robinson 2011) were complemented by dedicated interactions on the EU side. In 2012, the US Department of State hosted an EU-US workshop on critical infrastructure protection and SSA with representatives of the European Union (lead by Directorate General for Internal Market who was coordinating internally and other organs including the EEAS, EU Satellite Centre, and EDA, among others), as well as ESA on the US side including also the Department of Defense (Vittet-Philipp and Savova 2012, p. 4).

Discussions on developments continued in the EU community. A proposal for a SST framework was prepared (European Commission 2013a), which posited a governance model of European Member States and highlighted the potential benefits and security-related challenges. A dedicated impact assessment laid out the results of a consultation process and the conclusion already foreshadowed earlier that “European SST services” ought to be led by the EU rather than ESA (European Commission 2013b, p. 22). In exploring intergovernmental governance models other than those of the existing EU flagship programs, the assessment highlighted potential Member States for participation in a governance model (Next to FR, UK, and DE also IT and ES), who could bring sensors from the national side or developed as part of the framework of the ESA SSA preparatory program, but it also emphasized the need for dedicated networking and upgrading of hitherto separate capabilities (ibid, 2013b, p. 12–13). An initial appraisal of this work by the European legislative then considered different levels of engagement between Member States and EU organs (European Parliament 2013). The EU Satellite Centre, which was discussed as an entity contributing to service provision (European Parliament 2014, p. 11), had already been working on the exploration of potential elements related to the user interface of European SST services (Chatard-Moulin 2013, p. 12).

In view of a wider understanding of space-related risks, a nascent EU SST Support Framework was understood as a countermeasure to the emerging risk of space debris. It was added to the inventory of safeguards against risks to critical infrastructure (European Commission 2014a, p. 56) and highlighted as a necessity for the promotion of autonomy and security of European space-based services and for shared threat assessment (EU Global Strategy, 2016, p 42 and 45).

## Legal Basis

Finally, in 2014 the European Parliament and the Council adopted the legal basis establishing a “Framework for Space Surveillance and Tracking Support” (European

Parliament and European Council 2014). Articulating the need for a safe, secure, and sustainable orbital environment and the need for resilience of European space-based infrastructure, the decision aimed at “ensuring the long-term availability of European and national space infrastructure, facilities and services which are essential for the safety and security of the economies, societies and citizens in Europe” (Art. 3). To this end, a “SST capability at European level and with an appropriate level of autonomy” was to be put in place (Art. 4). This was to include the establishment and operation of three functions, including a “sensor function consisting of a network of Member State ground-based and/or space-based sensors, including national sensors developed through ESA, to survey and track space objects and to produce a database thereof”; a processing function to “process and analyze the SST data at national level to produce SST information and services for transmission to the SST service provision function”; and a service function that would provide collision avoidance, reentry, and fragmentation analysis services (Art. 5.1) to entities of the European Union, its organs, Member States, and industry (Art. 5.2) (see section “Users”).

Funding of 70 million Euros for a 5-year phase between 2016 and 2021 was set aside in parts from the Galileo and Copernicus funding streams for operational aspects, with additional funding earmarked for sensor upgrades from the EU research and development program, Horizon 2020, while significant previous investments of the participating Member States networking their assets were considered a prerequisite. The framework was designed not as an individual capability building exercise but as providing support to the networking and enhancement of existing and already emerging capabilities (That is until the start of the next so-called multiannual financial framework 2021–2027.).

## **A Consortium of European Member States in Cooperation with Council Agency**

In order to participate as sensor and service providers, Member States of the European Union with ownership of or access to requisite SST sensors were invited to express interest and apply to the European Commission via their so-called national designated entities (in most cases space agencies) and, upon demonstrating eligibility, to form a Consortium.

Subsequently, in response to Decision 541 of the European Council and the European Parliament (European Parliament and European Council 2014) and the related implementing decision (European Commission 2014b) that set out formal application procedures, five Member States applied (France, Germany, Italy, Spain, and the United Kingdom). Each of their respective national designated entities – space agencies or their equivalents (CNES, DLR, ASI, CDTI, and UKSA) – submitted individual applications to the European Commission for joint participation in the SST Support Framework, demonstrating compliance with the criteria set out in Decision 541 and security aspects (ibid, p. 3). After an assessment by the European Commission, the five applications were deemed compliant and proceeded,

according to the SST decision and implementing decision, to form a Consortium (European Commission 2014b).

A Consortium Agreement was signed by the heads of the participating space agencies in June 2015 (Via Satellite 2015; European Commission 2018a, p. 3). Encouraged by the decision, the partners of the SST Consortium collaborate with the EU Satellite Centre (EU SatCen), as an agency of the Council. An implementing arrangement was thus signed between the Consortium Member States and the EU SatCen in September 2015, thus formally constituting the SST Cooperation (ibid).

A tight timeframe between legal basis and proposed commencing of activities obliged the five-plus-one partners to proceed swiftly in setting up practical arrangements, applying formally for the requisite funding instruments earmarked by the European Union for this purpose, laying out technical activities for the initial services phase, and allocating resources among them in parallel (de Selding 2015). The activities were formally launched by the European Commission in January 2016 (European Commission 2018a, p. 3). This coincided with the aims set out in the 2016 Space Strategy, including a swift progression to reinforce and enhance the nascent SST activities further in view of the resilience of European space-based infrastructure (European Commission 2016, pp. 9–10).

A preparatory phase of six months focused on the fundamental coordination and preliminary joining of a distributed infrastructure, which involved the development of a service portfolio, an initial data and information policy, a model for internal burden-sharing in operations, the setup of front desk, and the acquisition of a first user cohort. Initial operations of the three SST services then commenced in July 2016 (European Commission 2018a, p. 4, 6; see also section “Services”).

As early as spring 2016, additional European Member States expressed an interest in joining the newly formed Consortium and started interactions. With an implementing act for an additional cohort adopted in late 2016, proceedings for the accession of further Member States commenced in 2017. Eleven Member States entered into a dialogue with the Consortium, of whom three decided to apply to the European Commission to join: Poland, Portugal, and Romania. They were found eligible in 2018 and formally completed the accession process with a fresh set of agreements in 2019. Eight other MS expressed an initial interest in participation in the SST Support Framework but refrained from an application to the Commission (European Commission 2018a, p. 8).

## Internal Governance

The SST Consortium is neither a legal entity nor an EU agency but constitutes a formal cooperation of the space agencies of the participating EU Member States. Despite different capabilities and legacies in the realm of SST, the partners agreed to commence their collaboration on quasi-equal footing with regard to voting rights and budget allocation, in order to cultivate a culture of cooperation and consensus necessary for joint efforts at the intersection of policy and operations.

The EU SST framework employs a novel governance model for space cooperation in Europe that differs from current governance models of communautized efforts or previously trialed public-private partnerships, of the main EU flagship programs for navigation, Galileo, and Earth observation, or Copernicus, which represented either new capabilities that formerly did not exist or were not available at the required scale.

The internal organization of the SST Cooperation (the Consortium and SatCen) includes three layers – decision-making, management, and working levels – that are jointly implemented by all partners in cross-agency teams. On the bottom level, the working level is structured into operational activities (see section “[Operations](#)”). A management layer coordinates the execution of the activities, handles administrative matters relating to finances, and grants and reports on administrative matters to European Commission and Research Executive Agency. On the decision level, the governance of the Consortium is executed through three committees: the Steering, Technical, and Security Committee. Each committee is formally staffed by two delegates from each Member State, in some cases a civilian lead from the participating space agency and a second representative from the armed forces or ministries of defense. The Security Committee handles all matters regarding data policy and security assessment and oversees matters relating to operational risk. The Technical Committee addresses all operational, research and development matters. Both committees provide direct input to the working and operational levels of SST that are organized as working groups for specific activities (Gravier and Faucher 2018).

The highest-level decision-making body of the Consortium is the Steering Committee, which is responsible for all aspects of policy and strategy, decides on budget allocation, and guides operational and technical activities. Its Chair and Secretariat – who do not represent their Member State in order to afford a degree of neutrality – are supported by a Co-Chair and maintain all external dialogue, both with the European Commission and international partners, and represent the SST Cooperation formally in the SST Committee. (The first chairmanship term was served by Germany from 2016 to mid-2017, co-chaired by the United Kingdom, followed by France from mid-2017 to 2020, co-chaired by Germany and the United Kingdom until end of 2018 and co-chaired by Germany since early 2019). The Steering Committee also forms the core of a dedicated forum for exchange with the SatCen (Coordination Committee) that addresses matters specifically to service provision and front desk activities. A representative of the European Commission usually observes the meetings of the Steering Committee. The committee meets usually monthly for several days, in some phases quasi fortnightly or weekly. It takes decisions by consensus but can vote with qualified majority to avoid impasse.

Several changes in the internal governance were initiated by the Consortium and the European Commission in the course of the first two years of operation. Beyond the formal accession procedure of new partners managed by the Commission, these included measures countering the complex funding arrangements that proved administratively cumbersome for both the European Commission and the partners (i.e., the regular reapplication for and simultaneous management of several 18-month-long grants across three budget lines). Initiated internally by the Consortium, voting rights

in the governance committees evolved from unanimity to qualified majority. The Consortium also facilitated a greater involvement of representatives of the European Commission in internal governance as observers in the Steering Committee since early 2017 (European Commission 2018a) and fundamentally changed the operational setup of the service provision model (see also section “[Services](#)”).

## Interaction with European Union Stakeholders

The European Commission is formally responsible for facilitation of the implementation of the framework, interacting through regular meetings with the SST Cooperation, drawing up relevant coordination plans, and monitoring the execution of the grants in collaboration with the EU’s Research Executive Agency (European Commission 2018a, p. 8). Due to the supplementary nature of the support framework – rather than a fully fledged program for now – the interaction between the SST Cooperation and its EU Stakeholders is not characterized by a classic customer relationship; notwithstanding, the SST Cooperation reports formally to the Commission and REA through the mechanisms associated with the funding instruments, as well as informally through regular, generally monthly meetings.

A further reporting line from the Consortium to its EU stakeholders – which surfaced as a fixture in the formal committee context when the Consortium became operational – is set up via the SST Committee. The SST Committee is a body of 28 EU Member States that monitors the implementation of the SST framework. Chaired by DG Grow, the committee serves as the forum for presentation, discussion, and adoption of proposals for the implementation of the SST framework. It usually involves briefings by the Commission, invites regular reports by the Consortium, and allows MS to discuss progress and initiatives. The forum regularly includes observers, both from EU organs (i.e., European External Action Service, European Defence Agency) or external entities in view of specific subject matter. Two further fora for SST experts and users allow for periodic discussion on specific topics relating to requirements and needs.

## Transatlantic Relationship

Since the first early exchanges between European and US stakeholders on emerging SSA capabilities in Europe, US actors have been observing the developments of European SSA closely. From a transatlantic perspective, engagement between Europe and the United States is constituted on three levels.

The Member States of the Consortium have each retained – some long-standing – bilateral relations with the United States, both through their space agencies and, crucially for SSA cooperation on policy and operational level, through their ministries of defense and armed forces (e.g., for data sharing arrangements and liaison officers, see also section “[Data Processing and Data Policy](#)”). These bilateral

relationships, in turn, extend to the multilateral level and form the engine for the transatlantic relationship between the SST Consortium as a whole and its US counterparts. As a multilateral group, the Consortium maintains a regular exchange on working level with representatives from the United States (cf. also section on STM). On supranational level, the EU-US space dialogue led by the European Commission does not yet regularly include EU SST representatives in its delegation but has grown to take into account the perspectives of EU SST for discussions related to SSA and STM, either by including relevant reporting through Commission officials or, more recently, through invitation of the chair of the Consortium per se.

---

## Operations

After a preparation period of 6 months from the activation of the financial instruments and budget lines, EU SST started providing operational services as a joint effort on 1 July 2016. While its governance is managed as a hybrid of virtual and co-located interaction, EU SST service provision is managed as a distributed European ground segment system incorporating the major functional elements set out in the legal basis of Decision 541.

### Service Provision Model Based on Internal Specialization

Operations consist of three main functions as per Decision 541, which make up the operational elements of the SST capability (i.e., aside from the governance elements described earlier): sensor, data processing, and service functions. SST sensors from all partners contribute data; this data is analyzed in the processing function and feed a joint database and ultimately a catalogue; from this, products are derived for three services that are generated by the operation centers and passed on to the users via a front desk.

In the interest of a swift progression to providing services to the EU user community after the entry into force of the legal basis in 2014 and the formation of the SST Consortium in 2015, the service provision model at the outset of operations in 2016 mirrored the equal footing approach of the participating partners: the CA service was operated on a fleet allocation principle, i.e., spacecraft or fleet was distributed to different operation centers (OCs), and services provided according a common guaranteed baseline with added-value elements at the discretion and capability of each operation center. At the time, RE and FG services were provided on a monthly rotational basis by all centers.

This provisional philosophy of each partner performing all functions was superseded in spring 2018 by an approach of specialization that is used to date, where each Consortium partner performs a pre-defined subset of the overall functions. Thus, pairs of OCs work in hot redundancy for the CA service, while all partners contribute offline and collaborate on post-analysis of events. The evolved service portfolio harmonizes products for all services. This internal burden-sharing constitutes a

model of functional specialization, whereby specific partners are responsible for European level service provision (the French and Spanish OCs for collision avoidance service, Italian OC for both reentry and fragmentation) and data processing side (German OC), while all individual partners contribute sensor data.

The current EU SST capability uses existing assets (sensors and operation centers) that are virtually coordinated and complemented through joint efforts in combining discrete elements into an overall value chain. Across the three functions, operations are led by the operation centers of the participating Member States (COO for France, GSSAC for Germany, UKSpOC for the United Kingdom, ISOC for Italy, S3TOC for Spain, SSAC-PL for Poland, COpE for Portugal, and COSST for Romania). These are civilian, military, or civilian-military and may integrate capabilities or expertise of additional actors of the SSA ecosystem in Europe, including industrial subcontractors or scientific institutes for development, staffing, or operation of selected infrastructure.

## Sensor Network

The EU SST sensor network has grown since initial operations, from 33 sensors in December 2017 of the initial Consortium of 5 partners (European Commission 2018a, p. 4) to a current total of 51 sensors made available for operations by its 8 partners. The network currently comprises of 12 radars (5 surveillance, 7 tracking), 35 telescopes (19 surveillance, 16 tracking), and 4 laser ranging stations. They provide coverage of all orbit regimes (LEO, MEO, HEO, and GEO) (European Commission 2018a, p. 4). The majority of sensors, including all radars and lasers, is located on European landmass (with the highest latitude site being Fylingdales in the United Kingdom); over a dozen additional telescopes afford coverage through locations in other geographical regions, including overseas territories or sites accessible through partners in the southern hemisphere. No space-based sensors are currently part of the system. Some Member State partners integrate assets or data from commercial or private entities (European Commission 2018a, p. 8). With the sensor network enlarged by additional Consortium partners, operational reviews are conducted annually to assess performance and contribution of each sensor.

The sensors operate at varying degrees of availability that are pre-defined and traded off among the partners. Control and tasking are retained by the respective Member States through their operation centers. On a network level, interactions are coordinated through the participating operation centers, which may send and receive tasking requests from other OCs and convene remotely for regular briefings.

The data provided from the sensors are shared either routinely in quasi real time or on request, depending on sensor type. They complement the data received through the 18th Space Control Squadron of the US Strategic Command in Vandenberg Air Force Base that are accessed through bilateral sharing agreements (for classified and nonclassified information). European measurements are thus systematically provided for the operation of each service, with dedicated campaigns performed for specific events: for collision avoidance services, in case of high-interest events

(HIE) and upon request of the nominal OC in charge of the service, all tracking radars and surveillance and tracking telescopes are activated to refine the orbit of the secondary object. For reentry services, upon request of the nominal OC, all tracking radars are activated to follow the reentry and provide European measurements; for fragmentation services, still upon request of the nominal OC, all radars and telescopes are tapped into according to their orbit regime.

## **Data Processing & Data Policy**

The data derived from the contributing sensors is shared according to pre-defined principles. For surveillance telescopes, data is shared on a daily basis; for tracking radars, tracking telescopes and lasers in quasi real time (daily or on request); and for surveillance radars on a daily basis.

During initial services, data exchange was performed manually between the operation centers. Today, the growing network of sensors, and the increase in European data necessitated a dedicated platform for the ingestion and exchange of data and for further processing in view of setting up a European catalogue. Measurements from the sensors are hence fed into, stored in, and shared via a common platform so-called European database. After development work, the database went operational in April 2019 and is hosted, in line with the service provision model of functional specialization, by one of the operation centers (German OC).

The database constitutes the basis for building and maintenance of the precursor European catalogue currently in development. The operation centers providing the SST services will use the European precursor catalogue for service provision, in complementation of CDM received from the United States.

One of the main challenges posited for the Consortium at the outset was the design of an effective data policy due to the sensitive domain of SSA (Marta 2015, p. 9 and 10). The data currently handled on a multilateral level inside the Consortium is not classified, while any required filtering is performed on the sensor side. For the sharing and exchange of data for operational purposes, the Consortium operates on the basis of a dedicated data and information policy drawn up prior to initial operations in 2016 and reviewed in 2018 by the requisite internal body, the Security Committee. Since 2019, a fresh review has been underway to revise the documents in view of the requirements posed by an enlarged Consortium with additional security constraints of the individual partners.

In absence of a multilateral sharing agreement, the architecture of existing bilateral arrangements relevant to the exchange of SSA data are being taken into account. The data and information policy specifically address interactions for the purposes of EU SST by the Consortium partners. Initiating and concluding general SSA data sharing arrangements are not within the remit of the Consortium but the prerogative of the individual partners' military and national security stakeholders.

All Consortium MS have general security agreements for the protection of classified material with each other, constituting the prerequisite for any exchange of classified documents or other material. In the past few years, all partners



concluded bilateral data sharing agreements with the United States for bilateral exchange of unclassified SSA data or are finalizing their respective arrangements (US STRATCOM 2019). France, Germany, and the United Kingdom have bilateral SSA data sharing agreements with the United States that also covers the exchange of classified SSA data, in addition to liaison officers of each of their respective Air Forces situated at the US Joint Force *Space* Component Command (*JFSCC*), formerly Joint Functional Component Command for *Space*, Vandenberg. Finally, two Member States of the Consortium, France and Germany, are currently the only partners to have concluded a bilateral SSA data sharing agreement with each other, covering the exchange of both unclassified and classified SSA data.

As approaches to data sharing are currently being further consolidated inside the Consortium, they must reconcile operational needs and individual security constraints with the features afforded by the evolving data processing function, and the general developments on a global level (i.e., developments on the US side with open architecture for data sharing; cf. also below for STM). Specific technical exercises on data sharing are therefore currently underway with relevant partners in the United States.

## Services

Since 2016, the SST Cooperation has been providing three operational SST services as outlined in the Decision 541: collision avoidance service, reentry analysis, and fragmentation analysis service.

The collision avoidance (CA) service is provided by the French and Spanish OCs (COO and S3TOC) operating in hot redundancy. Satellites or fleets of satellites are allocated when a user registers for the service via the front desk (see section “Users”). The CA service constitutes an added-value service, whereby several sources of data are used: conjunction data messages (CDM) from the United States and CDM generated autonomously from European sensor data, in addition to ephemeris provided by the spacecraft operator. The EU SST service complements US CDM through automatic acquisition, checks, and analysis of all incoming information; it provides alerts based on a threshold pre-defined by the registered user on three levels of risk (high interest, interest, information); and issues recommendations for avoidance maneuvers. Observation campaigns are conducted for high-interest events (HIE). There is direct interaction with the spacecraft operator to support decision-making as to whether to take an avoidance action. For LEO and GEO, timelines of identification of incoming risks, tasking requests to EU SST sensors and EU SST CDM generation, and notification of operators range from 7 to 14 days prior to the time of closest approach (TCA). Products provided to the operator include information on events, objects, miss distance, etc. They are complemented where needed, based on a dialogue with users, by mitigation recommendations, maneuver design, and maneuver support.

The reentry (RE) service is under the responsibility of the Italian Space Operations Centre (ISOC). It consists of two main products, a list of upcoming reentries and

reentry warning reports. Updated every 2–3 days, the list of upcoming reentries covers objects for which a reentry epoch within a period of up to 30 days has been computed, including object name, type, maximum latitude, size, and reentry prediction date range. Reentry warning reports are provided at least 3 days in advance of risky reentries and are updated as needed, including a final report to confirm the reentry. The user is actively notified and provided with information including details of the reentering object, estimated ground track, and uncertainty window.

The fragmentation (FG) service, also handled by ISOC, addresses fragmentations in orbit and consists of two products, a short-term and medium-term report. The short-term report is provided as soon as possible after a fragmentation event and includes the number of detected fragments and type of fragmentation. A medium-term report provides all additional available information including additional objects, orbit data, Gabbard diagram, and fragment cloud distribution and evolution. A current review of the fragmentation alert services foresees the addition of further features and a long-term analysis product of the event.

## Users

The products related to all three services are generated by the operation centers and passed on to the user through the service provision portal operated by the SST front desk, which is under the responsibility of the EU Satellite Centre. The services are free of charge, are available 24/7, and are currently accessible to European users, including organs of the European Union (European Commission and Council of the EU, European External Action Service), public and private spacecraft owners and operators, and European Member States and their research institutions, civil protection authorities, and space agencies. In view of some interest expressed by specific non-European users, discussions are ongoing on the oversight level of the program on EU level for potential future inclusion of external users.

Since the start of operations in July 2016, user uptake has grown to a current total of 104 registered users from 60 organizations in 18 EU Member States as of September 2019. The collision avoidance service has 43 registered users from 21 organizations (whereby, a small number are still completing the interface control documents related to the registration process). EU SST hence currently protects 129 spacecraft across all orbital regimes (40 in LEO, 30 in MEO, 59 in GEO) from the risk of collision. These users include European constellations such as the Galileo satellite navigation fleet, as well as fleets by commercial communications providers, military assets, and spacecraft operated by governmental entities. While some users use the products to corroborate existing processes, most integrated the SST collision avoidance service as an integral part into the value chain of routine operations (Monham 2018). For reentry analysis, there are 71 users from 47 organizations and for fragmentation analysis 60 users from 40 organizations.

As part of a so-called user interaction mechanism overseen by the European Commission and handled by the EU SatCen, regular user feedback is integrated in service portfolio development.

## Perspectives

Alongside the paradigmatic change in orbital utilization in the current decade, the global landscape of SSA is in the process of evolving significantly. As more actors bring various capabilities and interests to the table, elements such as governance and infrastructure come to the fore as key foci of international discourse in policy and operations (Lal et al. 2018). Security concerns have to be reflected on in light of post-Cold War practices of collaboration and transparency that have already overturned multilateral sharing practices in domains such as satellite imagery but must also cater to new risks and threats identified by major space-faring actors. Geographical opportunities for sensor sites and an array of cutting-edge and legacy sensor systems must be traded off with advanced operational needs of unprecedented orbital utilization, in order to define effective ground-based architectures. Moreover, the fusion, synthesis, and exchange of data and products from multiple sources need to be understood for SSA use cases that are likely to bifurcate broadly to include monitoring and coordination of large-scale orbital traffic on the one hand and the observation and verification of sophisticated proximity operations on the other.

At this point in time, European SST efforts also find themselves part of a dynamic debate close to home. As integration of SST capabilities is seen to take up speed (West 2018, p 11), the future of SSA capabilities in Europe and their operational, R&D, and political elements are being discussed on various levels including governmental (civilian and military programs and their bilateral partners), intergovernmental (European Space Agency), and – most crucially – supranational (European Union) levels.

## Evolution as a Sensor Network

As part of ongoing programmatic activities inside EU SST, the three main functions of sensors, data processing, and services are complemented by dedicated efforts for the upgrade and maintenance of sensors, in line with a vision for an enhanced architecture for the timeframe until 2028. With the recent enlargement of the Consortium to eight Member States, the network of operational radars, telescopes, and laser stations has already grown to include wider global coverage. As further participants may join the effort in the short- and midterm, the integration and trade-off of additional sensor assets and the targeted use of funds to support further developments are being assessed.

A fundamental part of this work consists of architecture studies currently being undertaken by the Consortium on request of the European Commission, with a focus on the sensor layer of the EU SST ground segment, in order to plan structured upgrades of specific sensors and optimize their use in the evolving sensor network between 2021 and 2028 (2021–2027 constitutes the upcoming budgetary timeframe of the multiannual financial framework of the European Union.). To this end, sensors – both existing and under development – are being examined as part of an added-value analysis, in order to determine an optimal architecture in view of possible

degrees of autonomy in different orbital regimes and prioritize sensors for upgrade accordingly. Specifically, the architecture studies involve the examination of several dozens of possible architectures until 2028, by simulating both sensor coverage and cataloguing performance, in view of a population of objects in orbit that evolves across time.

In consultation with the European Commission, these studies take into account the underlying philosophy of EU SST as a *support* framework that all but complements significant past and future investment of its Member States through funds for operation, maintenance, and upgrade, with limited EU co-funding assumed to consist of less than 50% in the future and two conservative budgetary scenarios of the upcoming EU space regulation (cf. next section). For GEO, a complete European autonomous surveillance capability for objects larger than 35 cm is feasible by 2028 with classical and wide field-of-view telescopes. For MEO, Europe could feasibly catalogue 80% of objects larger than 35 cm in the same timeframe. For LEO, Europe could be able to catalogue 9,000–11,000 objects larger than 7–10 cm by 2028 within the tentative budgetary constraints of the proposed EU space program.

Finally, while new sensor systems come online and legacy systems are due for upgrading in the short term, the Consortium is also set to lose valuable assets with the potential exit of the United Kingdom from the European Union. While this will signify the loss of a valued partner, the UK's interactions with the transatlantic SSA community have been long-standing. Since some partners of the SST Consortium actively engage in a range of multilateral space operations activities such as the Combined Space Operations (CSpO) initiative (US Air Force 2019), bi- and multilateral relations are likely to be maintained predominantly beyond the European Union SSA context.

## Evolution in the EU Space Program

The ongoing architecture studies are linked to the opportunities posed by the proposed space program of the European Union (European Commission 2018b). While its draft legal basis is yet to be completed, the overarching context is all but decided: the draft regulation foresees a maturation of the current EU SST Support Framework into a sub-component of a dedicated SSA program, a notion already foreshadowed in the call for enhancing the SST framework into a fully fledged SSA program in the European Space Strategy of 2016 (European Commission 2016, p. 10). The SSA program will be situated next to the flagship programs for Earth observation (EO) and position, navigation, and timing (PNT), as part of a dedicated package of new “security components,” which include SSA and Governmental Satellite Communications.

The SSA component is proposed to predominantly include SST, next to small-scale elements of space weather (SWE) and near-Earth objects (NEO), and will be furnished with a comparably minor share of the proposed overall 16 billion Euro budget. The current governance model of a Consortium or partnership of EU Member States – rather than a communautized program of all Member States

or a public-private partnership – is being affirmed and carried forward, with an opportunity for the accession of additional Member States of the European Union. The philosophy and mechanisms of internal governance remain largely unchanged. Indeed, certain elements proposed and implemented under the first two leadership terms of the current Consortium are being explicitly prescribed: these include functional specialization of key capability elements such as services or catalogue by a specific actor or tandem of actors, mechanisms that strengthen increased transparency, and involvement of representatives of the European Commission.

Given the dual aspect and increased security angle of the program, the context of EU SST in the evolving European ecosystem will be further complemented through instruments for cooperation put in place by the European Union in the defense domain such as the European Defence Fund (EDF), its precursor European Defence Industrial Development Program (EDIDP), and Permanent Structured Cooperation (PESCO). It remains a subject of discussion as to how these will be utilized by European actors to address SSA elements while avoiding duplication of key capabilities. Further developments will need to be seen in context also of recent national policies, such as the 2019 French Defence and Space Strategy, which posits SSA as a key domain, or the impending space policy of NATO that may manifest a need for a recognized space picture across a similar but different range of partners.

## Evolution in the Context of Space Traffic Management

In light of the emergence of large constellations with fleets of dozens, hundreds, or even thousands of spacecraft operated by private entities, the community of practice is increasingly discussing the notion of space traffic management (STM) or coordination. In absence of an unambiguous, shared definition of the concept among space-faring actors, the debate on STM gathers different perspectives that encompass technical and operational approaches linked to the exchange of data and information and to reflections on legal and regulatory aspects.

An emerging consensus in the discussion posits that on the one hand, STM activities will have to be addressed and implemented in the context of security political concerns that also impinge upon sovereign aspects (Becker 2019). On the other, future efforts in this evolving domain will also inevitably foot on a kind of multilateral or coordinated interaction between various global stakeholders (Lewis et al. 2018, p. 22 and 35). As the current SST framework is set to mature as part of the consolidation of the European space program in the coming decade, it will hence have to be seen in – and continue to consolidate its position within – the context of burden-sharing with transatlantic partners.

Recent developments in the United States saw the issuing of Space Policy Directive 3 (SPD-3) (Whitehouse 2018). SPD-3 proposes an integrated interagency approach towards STM. The US Department of Commerce is directed to act as a new civil focal point for public interface and on orbit SSA data sharing, while the US Department of Defense maintains the authoritative catalogue in view of its core national security mission. SPD-3 posits the main aspects of a space traffic

management regime, including SSA data, STM services, and STM science and technology, and also addresses national orbital debris mitigation policy, as well as global engagement. While the latter two, national regulation for space debris mitigation and global engagement for the promotion of norms of behavior, remain the remit of individual Member States, in Europe to date, it is the aspect of technical and operational STM that resonates most with EU SST. Essentially, the activities of EU SST as a civilian SSA actor today correspond to the technical and operational aspects of the STM initiative in the United States in view of data sharing through a repository (open architecture data repository in the United States and European database in the EU) and the provision of basic and added-valued services (e.g., collision avoidance).

In response to the US developments, the dialogue in Europe on STM has picked up momentum. It increasingly forges links between the current body of thinking on potential regulatory needs, existing operational and technological capabilities of government actors, and commercial entities that explored operational and governance aspects on SST (Tortora 2019). Senior representatives of the European Commission have described the Union's SST activities to constitute the basis for a future European STM regime (Bieńkowska 2019).

Finally, the shift of responsibilities of the US Department of Defense to the Department of Commerce will nevertheless leave bilateral agreements between military SSA actors that allow the current sharing of US CDM with Consortium Member States untouched. Beyond these fundamental bilateral channels between the United States and the individual EU SST Member States, the Consortium maintains a regular dialogue with US stakeholders from the Department of Defense, Department of State, and Department of Commerce in mutual pursuit of a collaborative approach.

---

## Conclusion

Space Surveillance and Tracking constitutes a fundamental capability to support and enable the operation of space-based services and assets. In view of foreseen activity in orbit of unprecedented scale, coupled with the growing criticality of – and risk to – space-based services, the domain of SSA will be salient in the mid- and long term. It will likely be pursued both by those state actors that operate their own maneuverable space assets and have a primary interest safeguarding them, and by state and non-state actors that can bring pertinent technology and infrastructural elements to the table.

In its comparatively short history, the implementation of the EU Space Surveillance and Tracking Support Framework has seen the convergence of a diverse group of stakeholders in a novel model for space cooperation in Europe. For some Member States, the inception of EU SST presented an opportunity to foster nascent engagement and interest in the domain of SSA; for others it serves as a multilateral forum to draw on existing rich legacies and make those available to the wider community. By employing a communal but tailored bottom-up approach to an SST system, EU SST allowed for a comparably rapid progression to fundamental operational services

while honoring long-standing security constraints articulated by its key actors. A streamlined governance enables leverage for both the European Union and those state actors with long-standing operational and political investment in the SSA domain, and at the same time encourages increased participation by those state actors who begin to recognize SSA as an important field. It allows the contribution of industry actors to those parts of the SSA value chain deemed meaningful and effective by individual governmental actors while binding the latter in a joint effort of cooperation.

Borne out of the need to advance a strategic capability for the European community, EU SST hence constitutes an effort to consolidate and enhance capabilities of traditional and emerging space actors, as well as an exercise in transparency building within and beyond Europe. In fusing external data from the United States with that of an expanding distributed sensor network operated by European actors, SST services are provided free of charge to an increasingly large user community in Europe that includes commercial, governmental, and intergovernmental users who operate fleets of spacecraft or handle civil protection. Through an approach of layered dependencies among the Member States contributing to EU SST in Europe and as a European collective vis-à-vis transatlantic partners, the framework advances global burden-sharing of safeguarding strategic space assets. It also ties into the efforts of promoting the sustainability of the orbital environment and constitutes a building block for future operational activities in the area of space traffic management and coordination.

As integral component of the planned European Union space program, European SST activities are set to mature into a program in their own right, with an enhanced catalogue, services, and a globally distributed sensor architecture that affords greater levels of autonomy across orbital regimes. As such, the evolution of the SST capability of the European Union must be observed in the context of capabilities of global activity: like other major efforts, it faces the challenge and opportunity to slot into the global ecosystem of different governmental and commercial actors developing and operating existing and next-generation SSA capabilities; it contributes to the contemporary dialogue of global community on how to ingest of multiple sources of data and process for meaningful, actionable products; and must convene in organizational frameworks that take into account the different contributions and requirements of a highly diverse community.

---

## References

- Becker M (2019) Kein Krieg der Sterne, *Internationale Politik*, January/February 2019, 62–67
- Bieńkowska E (2019) Keynote speech at 35th space symposium, Colorado Springs, 10 April 2019. [https://europa.eu/rapid/press-release\\_CLDR-19-2012\\_en.htm](https://europa.eu/rapid/press-release_CLDR-19-2012_en.htm). Accessed 17 July 2019
- Chatard-Moulin P (2013) Horizon 2020 work programme, horizon 2020 space information day, Brussels, 11 December 2013. European Commission, Brussels
- Chow T (2011) Space situational awareness sharing program. Secure World Foundation, Washington DC

- Commission of the European Communities (2003) Space: a new European frontier for an expanding union: an action plan for implementing the European space policy (white paper), COM(2003) 673. Commission of the European Communities, Brussels
- Council of the European Union (2011) High-level SSA civil-military use requirements. European External Action Service, Brussels
- Council Resolution (2008) Taking forward the European space policy. Council of the European Union, Brussels
- Council Resolution (2010) Global challenges: taking full benefit of European space systems. Council of the European Union, Brussels
- de Selding PB (2015) A European space surveillance network inches forward. Spacenews, 17 June 2015 (online). <https://spacenews.com/a-european-space-surveillance-network-inches-forward/>. Accessed 17 July 2019
- Dickow M (2015) The pursuit of collective autonomy? Europe's autonomy in "space and security" lacks a joint vision. Al-Ekabi C (ed) European autonomy in space. *Stud Space Policy* 10:113–123
- Donath T, Schildknecht T, Martinot V, Del Monte L (2009) Possible European systems for space situational awareness. *Acta Astronaut* 66(2010):1378–1387
- EDA (2010) EDA common staff target, 25 march 2010 (EDA SBD 2010–07). European Defence Agency, Brussels
- ESA (2008) Space situational awareness preparatory programme proposal ESA/C(2008)142. European Space Agency, Paris
- ESPI (2018) Security in outer space: rising stakes in Europe. European Space Policy Institute, Vienna
- European Commission (2013a) Proposal for a decision of the European parliament and of the council establishing a space surveillance and tracking support programme. European Commission, Brussels
- European Commission (2013b) Commission staff working document: impact assessment accompanying the document proposal for a decision of the European parliament and of the council establishing a space surveillance and tracking support programme, SWD(2013)55 final. European Commission, Brussels
- European Commission (2014a) Commission staff working document: overview of natural and man-made disaster risks in the EU SWD(2014) 134. European Commission, Brussels
- European Commission (2014b) Commission implementing decision of 12.9.2014 on the procedure for participation of the member states in the space surveillance and tracking support framework, C(2014)6342. European Commission, Brussels
- European Commission (2016) A space strategy for Europe, COM(2016) 705. European Commission, Brussels
- European Commission (2018a) Report from the commission to the European parliament and the council on the implementation of the space surveillance and tracking (SST) support framework (2014–2017), COM(2018)256. European Commission, Brussels
- European Commission (2018b) Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the space programme of the union and the European Union Agency for the space programme. European Commission, Brussels
- European Parliament (2013) Initial appraisal of a European commission impact assessment: European commission proposal for a decision of the European parliament and of the council establishing a space surveillance and tracking support programme. European Parliament, Brussels
- European Parliament (2014) Position of the European parliament adopted at first reading on 2 April 2014 with a view to the adoption of decision no .../2014/EU of the European parliament and of the council establishing a framework for space surveillance and tracking support, EP-PE\_TC1-COD(2013)0064, European Parliament, Brussels
- European Parliament and European Council (2014) Decision No 541/2014/EU of the European Parliament and of the Council of 16 April 2014 establishing a Framework for Space Surveillance and Tracking Support, Official Journal of the European Union, 27.5.2014, Brussels



- Flohner T, Krag H (2017) Space surveillance and tracking in ESA's SSA programme. In Proceedings of the 7th European conference on space debris, Darmstadt, 18–21 April 2017
- Gravier A, Faucher P (2018) EU Space surveillance & tracking support framework: a consortium of member states safeguarding European space infrastructure & orbital environment, IFRI conference: La sécurité de l'espace dans les années 2020: perspectives transatlantiques, 27 November 2018, Bruxelles
- Lal B, Balakrishnan A, Caldwell BM, Buenconsejo RS, Carioscia SA (2018) Global trends in space situational awareness (SSA) and space traffic management (STM). Institute for Defense Analysis, Washington D.C.
- Lewis P, Parakilas J, Schneider-Petsinger M, Smart C, Rathke J, Ruy D (2018) The future of the United States and Europe: an irreplaceable partnership. Chatham House and Center for Strategic & International Studies, London/Washington D.C.
- Marta LC (2015) The European space surveillance and tracking service at the crossroad. *Def Ind* 5:9–11
- Marta LC, Gasparini G (2008) Europe's approach space situational awareness. In: Schrogl K-U, Mathieu C, Peter N (eds) *Yearbook on space policy 2007/2008: from policies to programmes*. Springer, New York, pp 138–151
- Mazurelle F, Wouters J, Thiebaut W (2009) The evolution of European space governance: policy, legal and institutional implications. *Int Organ Law Rev* 6:155–189
- McCormick PK (2013) Space debris: conjunction opportunities and opportunities for international cooperation. *Sci Public Policy* 40(6):801–813
- McCormick PK (2015) Space situational awareness in Europe: the fractures and the federative aspects of European space efforts. *Astropolitics* 13:43–64
- Monham A (2018) Securing EUMETSAT's mission from an evolving space environment 12th ESPI autumn conference, 27–28 September 2018. European Space Policy Institute, Vienna
- Nardon L (2007) Space situational awareness and international policy (document de travail 14). l'Institut français des relations internationales (IFRI), Paris
- Pagkratis S (2011) European space activities in the global context. In: Schrogl KU, Pagkratis S, Baranes B (eds) *Yearbook on space policy 2009/2010: space for society*. ESPI/Springer, Vienna, pp 2–132
- Pasco X (2008) Study on suitable governance and data policy models for a European Space Situational Awareness (SSA) system. Fondation pour la Recherche Stratégique, Paris
- Pasco X (2009) A European approach to space security. American Academy of Arts and Sciences, Cambridge, MA
- Pellegrino M, Stang G (2016) Space security for Europe. EUISS report no. 29, July 2016. EU Institute for Security Studies, Paris
- Robinson J (2011) Space security for the transatlantic partnership: conference report and analysis, report 38, November 2011. European Space Policy Institute (ESPI), Vienna
- Rovetto RJ, Kelso TS (2016) Preliminaries of a space situational awareness ontology, advances in the astronautical sciences, preprint AAS 16–510
- SPASEC (2005) Report of the panel of experts on space and security (issue 1.12). European Commission, Brussels
- Tortora JJ (2019) Space traffic management: a long way ahead. *J Space Saf Eng* 6(2):69
- US Air Force (2019) Multinational statement for combined space operations, 10 April 2019 (online). <https://www.afspc.af.mil/News/Article-Display/Article/1810793/multinational-statement-for-combined-space-operations/>. Accessed 17 July 2019
- US Strategic Command (2019) USSTRATCOM, polish space agency sign agreement to share space services, data, US strategic command public affairs, 11 April 2019, <https://www.stratcom.mil/Media/News/News-Article-View/Article/1811729/usstratcom-polish-space-agency-sign-agreement-to-share-space-services-data/>. Accessed 17 July 2019
- Veclani AC, Sartori N, Battisti E, Darnis JP, Cesca E (2014) Space, sovereignty and European security: building European capabilities in an advanced institutional framework. Directorate-General for External Policies, European Parliament, Brussels

- 
- Via Satellite (2015) Five European countries sign space surveillance and tracking agreement, satellite today, 17 June 2015 (online), <https://www.satellitetoday.com/government-military/2015/06/17/five-european-countries-sign-space-surveillance-and-tracking-agreement/>. Accessed 4 July 2019
- Vittet-Philipp P, Savova T (2012) International research update, issue 23, Brussels. European Commission, Brussels
- West J (2018) Space security index 2018. Project Ploughshares, Waterloo
- Whitehouse (2018) Space policy directive-3, national space traffic management policy. Office of the President of the United States, Washington DC



# China's Capabilities and Priorities in Space-Based Safety and Security Applications

# 47

Lin Shen, Hongbo Li, Shengjun Zhang, and Xin Wang

## Contents

Introduction .....	906
China's Space Safety and Security Policy .....	906
Analysis of China's Capabilities in Space Safety and Security .....	907
Earth Observation (EO) .....	907
Communication Satellites .....	910
Satellite Positioning, Navigation, and Timing System .....	912
Space Situation Awareness .....	914
International Exchanges and Cooperation on China's Space Safety and Security .....	916
Conclusion .....	918
References .....	918

## Abstract

China's space industry has developed considerably since it was first established in 1956. Following a strategy based on self-reliance, China relies primarily on its own capabilities to develop space industry to meet the needs of modernization, based upon its actual conditions and strength. Significant achievements in the fields of Earth observation (EO), communication satellite system, positioning, navigation and timing (PNT), and space situational awareness (SSA) have been realized.

L. Shen · H. Li (✉) · S. Zhang · X. Wang  
China Academy of Launch Vehicle Technology (CALT), Beijing, China  
e-mail: [tolinsh@sina.com](mailto:tolinsh@sina.com); [lhbospace@sina.com](mailto:lhbospace@sina.com); [zhangsj98@sina.com](mailto:zhangsj98@sina.com); [wangxin.1122@163.com](mailto:wangxin.1122@163.com)

## Introduction

China space industry has developed fast since it was established in 1956. Over the past 60 years, achievements include the development of atomic and hydrogen bombs, missiles, man-made satellites, and a lunar probe. China has also achieved manned spaceflight. China is unflinching in pursuing the road of peaceful development, while maintaining that outer space is the common wealth of mankind. While supporting all activities that utilize outer space for peaceful purposes, China actively explores and uses outer space and continuously makes new contributions to the development of manned space programs (The State Council Information Office of the People's Republic of China 2006).

China has contributed largely to some of the world's most advanced technologies in many important fields, including satellite recovery, multi-satellite launch, Cryogenic fuel rocket technology, cluster carrier rocket technology and geostationary Earth orbit (GEO) satellite launch, telemetry, and Tracking and Command (TT&C). China has also made significant achievements in the development and application of remote sensing satellites, communication satellites, and BeiDou Navigation Satellite System (The State Council Information Office of the People's Republic of China 2000). Space science, technologies, and applications have achieved fruitful results.

---

## China's Space Safety and Security Policy

Space is the commanding point of international strategic competition. The weaponization of space emerged as a result of the development of space forces and means by some countries (The State Council Information Office of the People's Republic of China 2015).

China's policy advocates for the peaceful use of space and against the weaponization of space and the arms race in space. As such China is actively participating in international space cooperation. Closely following the space situation, the country monitors the threats and challenges of space security, while it safeguards the security of space assets, serves national economic construction and social development, and maintains space security.

China takes a defensive posture in the frame of its national defense policy, and its development does not pose a threat to any country. No matter how far China develops, it will never seek hegemony. The purpose of China's space development is to explore outer space and enhance the understanding of the Earth and the cosmos; to utilize outer space for peaceful purposes, promote human civilization and social progress, and benefit the whole of mankind; to meet the demands of economic, scientific, and technological development, national security, and social progress; and to improve the scientific and cultural levels of the Chinese people, protect China's national rights and interests, and build up its overall strength. (The State Council Information Office of the People's Republic of China 2016).

According to its policy, China's space industry is subject to and serves the national overall development strategy and adheres to the principles of innovative, coordinated, peaceful, and open development.

1. Innovative development. China takes independent innovation as the core of the development of its space industry. It implements major space science and technology projects, strengthens scientific exploration and technological innovation, deepens institutional reforms, and stimulates innovation and creativity, working to promote rapid development of the space industry.
2. Coordinated development. China rationally allocates various resources and encourages and guides social forces to take an orderly part in space development. All space activities are coordinated under an overall plan of the state to promote the comprehensive development of space science, space technology, and space applications and to improve the quality and efficiency of overall space development.
3. Peaceful development. China always adheres to the principle of the use of outer space for peaceful purposes and opposes the weaponization of outer space or an arms race in outer space. The country develops and utilizes space resources in a prudent manner and takes effective measures to protect the space environment to ensure a peaceful and clean outer space and guarantee that its space activities benefit the whole of mankind.
4. Open development. China persists in combining independence and self-reliance with opening to the outside world and international cooperation. It actively engages in international exchanges and cooperation on the basis of equality and mutual benefit, peaceful utilization, and inclusive development, striving to promote progress of space industry for mankind as a whole and its long-term sustainable development.

Since 2000, the Information Office of the State Council has published a space white paper every 5 years. So far, four space white papers have been published. The latest one was issued in 2016. The white papers offer a brief introduction about China's space development objectives, vision and principles, recent space progress, future space plans, development policies and measures, and international exchanges and cooperation.

---

## **Analysis of China's Capabilities in Space Safety and Security**

### **Earth Observation (EO)**

On April 24, 1970, China successfully developed and launched the first man-made Earth-orbiting satellite, Dongfanghong-1, and became the fifth country in the world to independently develop and launch man-made satellites. China is the third country in the world to master satellite recovery technology. The success rate of satellite recovery has reached the international advanced level. The use of the Fengyun

(wind and cloud), Haiyang (ocean), Ziyuan (resources), Gaofen (high-resolution), Yaogan (remote sensing), and Tianhui (space mapping) satellite series and constellation of small satellites for environment and disaster monitoring and forecasting has been improved. (The State Council Information Office of the People's Republic of China 2016).

### **Fengyun Satellite Series**

As early as the 1970s, China began to develop its meteorological satellites. Since then, 17 meteorological satellites have been launched. China is the third country after the United States and Russia to have polar orbiting meteorological satellites and geostationary Earth-orbit meteorological satellites at the same time (National Satellite Meteorological Center 2019).

Under the coordination and management of the World Meteorological Organization (WMO), all countries in the world have achieved the goal of exchanging meteorological observation data and acquiring global meteorological observation data. The Global Operational Meteorological Satellite Detection System (GOMSS) is a space-based detection system built through the joint efforts of countries launching and operating meteorological satellites under the coordination of WMO. China's operational meteorological satellites Fengyun-3, Fengyun-2, and Fengyun-4A have become important members of the global operational meteorological satellite detection system. They supplement each other in coverage and resolution and help China acquire global information and monitor regional disastrous weather and environmental and meteorological services, as well as Earth sciences.

### **Ocean Satellite Series**

The first "Ocean" dynamic and environmental environment sensing satellite was launched in August 2011 (The State Council Information Office of the People's Republic of China 2011). It has the capability of all-weather and full-time observation in microwave region. The Haiyang-2 satellite is capable of all-weather, full-time, and high-accuracy observation of marine dynamic parameters such as sea height, sea wave, and sea surface wind. (The State Council Information Office of the People's Republic of China 2016).

China is developing three ocean monitoring satellites: color environment satellite (HY-1), ocean power ocean dynamic environment satellite (HY-2), and ocean radar satellite (HY-3). The system will realize product diversification, data standardization, application quantification, and operational operation and will meet increasing global requirements for ocean surveillance and monitoring. It also provides strong technical support for the implementation of marine development strategies. The system effectively implements marine environment and resources monitoring and provides services for the protection of marine rights and interests, disaster prevention and mitigation, and national economic construction by improving the accuracy and timeliness of marine environment forecasting and marine disaster early warning, (National Satellite Oceanic Application Center 2012).

### **Ziyuan Satellite Series**

China has successively launched Ziyuan-1, Ziyuan-2, and Ziyuan-3. Until now, Ziyuan-3 01 and 02 stereo mapping satellites have achieved double star networking and operating. ZY-3 01 is the first high-resolution optical transmission stereo mapping satellite in China. It was successfully launched on January 9, 2012. It integrates mapping and resource investigation functions. ZY-3 02 was successfully launched on May 30, 2016. It is a high-resolution stereo mapping operational satellite. It is optimized on the basis of ZY-3 01 and carries payloads such as a three-line array mapping camera and a multispectral camera. The resolution of front and rear viewing cameras is improved from 3.5 m to better than 2.5 m. It also carries a set of experimental laser altimetry payload. The performance achieved is better than the ZY-3 01 satellite in image fusion ability and elevation measurement accuracy (Land Satellite Remote Sensing Application Center 2019).

### **Gaofen Satellite Series**

China is building a high-resolution Earth observation system-of-system based on satellite imagery and stratospheric airships and aircraft, improving the corresponding ground systems and establishing data and application centers. Combined with other observation means, the system will form an all-weather, all-time, and global coverage Earth observation capability. By 2020, an advanced terrestrial, atmospheric, and oceanic Earth observation system will be built to provide services and assist in decision making processes for important fields such as modern agriculture, disaster reduction, resources and environment, and public safety.

The first Gaofen-1 satellite was launched on April 26, 2013. It combines high resolution and wide swath width, with a designated life span of 5–8 years (China National Space Administration 2019). The satellite is widely used in the fields of land and resources, environmental protection, precision agriculture, disaster prevention, and mitigation. Gaofen-2 achieves submeter optical remote sensing. Gaofen-3 is a SAR satellite and achieves 1 meter resolution. Gaofen-4 is China's first GEO high-resolution Earth observation satellite.

### **Environment and Disaster Monitoring and Forecasting Small Satellite Constellation**

The HJ-1A/B/C environment and disaster monitoring and forecasting small satellite constellation includes two optical satellites, HJ-1A/B and one radar satellite HJ-1C, which can carry out large-scale, all-weather, and 24 h dynamic monitoring for ecological environment and disaster. These satellites are equipped with four remote sensors such as wide-coverage CCD scanner, infrared multispectral scanner, hyperspectral imager, and synthetic aperture radar, comprising a more complete Earth observation remote sensing series characterized by high and medium space resolution, high time resolution, high spectrum resolution, and wide coverage (China Centre for Resources Satellite Data and Application 2019).

## **Commercial Earth Observation**

In 2015, the first satellite of China's first commercial remote sensing constellation, Jilin-1, was launched. In early 2018, four satellites of Gaojing-1 formed the first commercial remote sensing constellation with 0.5-meter resolution in China.

China established a ground data processing system for Earth observation satellites, common application supporting platform, and multilevel network data distribution system. Such capabilities greatly enhance China's abilities in data processing, archiving, distribution, services provision, and quantitative applications. Industrial application system-building is in full swing, having completed 18 industrial and two regional application demonstration systems, and set up 26 provincial-level data and application centers. An integrated information service sharing platform for a high-resolution Earth observation system has been built. Earth observation satellite data is now widely used in industrial, regional, and public services for economic and social development.

In the future, in accordance with the policy guideline for developing multifunctional satellites, and creating networks of satellites and integrating them, China will focus on three series of satellites for observing the land, ocean, and atmosphere, respectively. China is to develop and launch satellites capable of high-resolution multi-mode optical observation, L-band differential interferometric synthetic aperture radar imaging, carbon monitoring of the territorial ecosystem, atmospheric Lidar detection, ocean salinity detection, and new-type ocean color observation. China will take steps to build highly efficient capabilities of its own, comprehensive global observation and data acquisition with a rational allocation of low-, medium- and high-spatial resolution technologies and an optimized combination of multiple observation methods.

## **Communication Satellites**

China is the fifth country in the world to independently develop and launch GEO communication satellites. Currently, China's aerospace industry has mastered key technologies in public platform of large-capacity GEO satellites, space-based data relay, and TT&T. The performance of satellites has been significantly improved, and the level of voice, data and radio, television communication, and broadcasting has been further improved. The successful launch of communications satellites such as Yatai and Zhongxing represent the completion of a fixed communications satellite support system whose communications services cover all of China's territory as well as major areas of the world. The successful launch and stable operations of the Zhongxing 10 satellite have greatly increased the power and capacity of China Telecom and Broadcasting Satellite. The Tiantong-1, China's first mobile communications satellite, has been successfully launched. The first-generation data relay satellite system composed of three Tianlian-1 satellites has been completed, and high-speed communication test of satellite-ground laser link has been crowned with success. The Shijian-13 satellite launched in 2017 will realize the broadband application of autonomous communication satellites and promote the development of



China's satellite communication industry. The Ka-band multi-beam broadband communication system on this satellite is the first application in domestic communication satellite. It can support multiuser and large capacity bidirectional using and download data at high speed through this satellite while supporting a large number of users to upload data at high speed in vast areas. The satellite breaks through a series of technical problems such as Ka multi-beam broadband system design, antenna reflector profile accuracy control and measurement, antenna pointing accuracy calibration, and so on. The related technology has reached the international advanced technology level (XINHUANET 2019).

By the end of 2016, China has developed three generations of Dongfanghong series communication satellite platform. Dongfanghong-4 platform is the main platform in service. The fourth generation Dongfanghong-5 super-large capacity platform is being developed.

Since the mid-1980s, China has developed satellite communication technology by using domestic and foreign communication satellites to meet the growing needs of communication, broadcasting, and education. For fixed satellite communication services, dozens of large and medium satellite communication Earth stations have been built throughout the country, with more than 27,000 international satellite communication lines connecting more than 180 countries and regions in the world. China has built a domestic satellite public communication network, with more than 70,000 domestic satellite communication telephone routes, and initially solved the communication problems in remote areas. Very small aperture terminal (VSAT) communication business has developed rapidly in recent years. There are 30 domestic VSAT communication business units serving 15,000 small station users, including more than 6,300 bidirectional small station users. At the same time, more than 80 special communication networks of finance, meteorology, transportation, petroleum, water conservancy, civil aviation, power, health, and journalism departments have been established, including tens of thousands VSAT. For satellite television broadcasting business, China has built a satellite television broadcasting system covering the whole world and a satellite television education system covering the whole country. Since 1985, China has used satellite to transmit radio and television programs. At present, it has formed a satellite transmission coverage network, which occupies 33 communication satellite transponders. It is responsible for transmitting 47 sets of central and local TV programs and educational TV programs, as well as 32 channels of internal and external broadcasting programs and nearly 40 sets of local broadcasting programs. Over the past 10 years since the launch of satellite education television broadcasting, more than 30 million people have received education and training in colleges and secondary schools. In recent years, the nation has built a satellite live broadcasting test platform, which transmits satellite TV programs from central and local governments to vast rural areas that are not covered by radio and television through digital compression, thus greatly improving the coverage of radio and television in China. There are about 189,000 satellite TV broadcasting stations in China. On the satellite live broadcasting test platform, a broadband multimedia transmission network of China's educational satellite has been established to provide comprehensive services of distance education and information technology for the whole country.

In the future, China will be oriented toward industrial and market applications and mainly operates through business models while meeting public welfare needs. China will develop both fixed and mobile communications and broadcasting as well as data relay satellites and build a space-ground integrated information network consisting of space-based systems such as high-Earth-orbit broadband satellite systems and low-Earth-orbit mobile satellite systems and ground-based systems such as satellite-access stations. TT&C stations, gateway stations, uplink stations, calibration fields, and other satellite ground facilities are to be built synchronously. These efforts are expected to bring about a comprehensive system capable of providing broadband communications, fixed communications, direct-broadcast television, mobile communications, and mobile multimedia broadcast services. A global satellite communications and broadcasting system integrated with the ground communications network will be established step-by-step.

## **Satellite Positioning, Navigation, and Timing System**

Satellite navigation system is an indispensable information infrastructure for national security and economic and social development. The BeiDou Navigation Satellite System (BDS) has been independently constructed and operated by China with an eye to the needs of the country's national security and economic and social development. As a space infrastructure of national significance, BDS provides all-time, all-weather, and high-accuracy positioning, navigation, and timing services to global users (China Satellite Navigation Office 2018).

China attaches great importance to the BDS construction and development. In 2013, "the Medium and Long-Term Development Plan for the National Satellite Navigation Industry" was released, to make overall arrangement for medium and long-term satellite navigation industrial development and to provide the guidance of macro policies. In 2016, "China's BeiDou Satellite Navigation System," a governmental white paper, was released, to introduce the BDS development methods and policies.

Navigation satellite systems are public resources shared by the whole globe, while the multi-system compatibility and interoperability have become a trend. China has been applying the principle that "BDS is developed by China, and dedicated to the world," serving the development of the Silk Road Economic Belt and actively pushing forward international cooperation related to BDS. As BDS joins hands with other navigation satellite systems, China works with all other countries, regions, and international organizations to promote global satellite navigation development and make BDS further serve the world and benefit mankind.

BDS possesses the following characteristics: first, its space segment is a hybrid constellation consisting of satellites in three kinds of orbits. In comparison with other navigation satellite systems, BDS operates more satellites in high orbits to offer better anti-shielding capabilities, which is particularly observable in terms of performance in the low-latitude areas. Second, BDS provides multi-frequency navigation signals with which can be combined to improve service accuracy. Third, BDS

integrates navigation and communication capabilities and has multiple service functions including real-time navigation, rapid positioning, precise timing, location reporting, and short message communication services.

BDS is mainly comprised of three segments: a space segment, a ground segment, and a user segment. The BDS space segment is a hybrid navigation constellation consisting of geostationary Earth orbit (GEO), inclined geosynchronous satellite orbit (IGSO), and medium Earth orbit (MEO) satellites. The BDS ground segment consists of various ground stations, including master control stations, time synchronization/uplink stations, monitoring stations, as well as operation and management facilities of the inter-satellite links. The BDS user segment consists of various kinds of basic BDS products, including chips, modules, and antennae as well as the BDS terminals, application systems, and application services, which are compatible with other systems. Relevant products of BDS have been widely used in transportation, marine fisheries, hydrological monitoring, meteorological forecasting, surveying and mapping geographic information, forest fire prevention, communication time unification, electric power dispatch, disaster relief and mitigation, emergency rescue, and other fields.

In the late twentieth century, China started to explore a path to develop a navigation satellite system suitable for its national conditions, and gradually formulated a three-step development strategy. The first step is to construct BDS-1. The project started in 1994 and was ready to operate in 2000, with the launch of two GEO satellites. With an active-positioning scheme, the system provided users in China with positioning, timing, wide area differential, and short message communication services. The third GEO satellite was launched in 2003, which further enhanced the system performance. The second step is to construct BDS-2. The project started in 2004, and by the end of 2012, a total of 14 satellites, including 5 GEO satellites, 5 IGSO satellites, and 4 MEO satellites, had been launched to complete the space constellation deployment. Besides a technical scheme which was compatible with BDS-1, BDS-2 added the passive-positioning scheme and provided users in the Asia-Pacific region with positioning, velocity measurement, and timing as well as short message communication services. The third step is to construct BDS-3. The project started in 2009, and by the end of 2018, a total of 19 satellites were launched to complete a preliminary system for global services. It is planned to comprehensively complete the deployment of BDS-3 with the launching of 30 satellites by around 2020. BDS-3 has inherited the technical schemes of both active and passive services, and can provide basic navigation (including positioning, velocity measurement and timing), global short message communication, and international search and rescue services to global users. Users in China and surrounding areas can also enjoy regional short message communication, satellite-based augmentation, and precise point positioning services, etc.

Until now, the construction BeiDou-2 system has been completed, with the networking of 14 BeiDou navigation satellites, officially offering positioning, velocity measurement, timing, wide area difference, and short-message communication service to customers in the Asia-Pacific region. BeiDou's global satellite navigation system is undergoing smooth construction. By the end of 2018, a total of 19 satellites

were launched to complete a preliminary system for global services. Around 2020, the BDS-3 will be deployed with the launching and networking of 30 satellites.

In the future, BDS will continue to improve the service performance, to expand the service functions, and to enhance continuous and stable operation capability. Before the end of 2020, BDS-2 will launch 1 backup GEO satellite; BDS-3 will launch another 6 MEO, 3 IGSO, and 2 GEO satellites, to further improve the global basic navigation and regional short message communication service capabilities, and to realize the global short message communication, satellite-based augmentation, international search and rescue, and precise point positioning service capabilities, etc.

## Space Situation Awareness

China advocates strengthening international space communication and cooperation and promoting inclusive development based on equality and mutual benefit, peaceful use, and common development. In order to achieve the goal of peaceful development and utilization of outer space and effectively safeguard space security, China will, on the basis of adhering to the principle of peaceful development and utilization of outer space and in full cooperation with the international community, especially developing countries, continue its opposition to the weaponization of outer space and the arms race in outer space, strive for the equal exploitation and peaceful use of outer space resources, and promote the establishment of a new international space order. It will make greater contributions to promoting economic development and social progress, safeguarding space security and world peace.

Space debris is the waste abandoned in space by human beings in space activities, also known as “space garbage.” It mainly includes abandoned spacecraft and launch vehicle rockets, solid rocket burners, debris generated by spacecraft on-orbit operation and collision disintegration, etc. At present, there are hundreds of millions of space debris above the millimeter level, with a total mass of several thousand tons. The average impact velocity of space debris is 10 km per second. Space debris above centimeter level can lead to complete damage of spacecraft, while the cumulative impact effect of millimeter or micron level space debris will lead to performance degradation or function failure of spacecraft. According to statistics, China’s on-orbit spacecraft has reached more than 270, with an average of more than 30 close-range dangerous rendezvous with space debris within 100 m per year. In addition, many space debris return to the atmosphere every year. These frequent meteoric events have posed a serious threat to the safety of ground personnel and property.

Space debris poses the greatest threat to space activities; thus, China will continue to strengthen space debris monitoring, mitigation, and spacecraft protection. China will develop technologies for monitoring space debris and pre-warning of collision and begin monitoring space debris and small near-Earth celestial bodies and collision pre-warning work. It will set up a design and assess system of space debris mitigation and take measures to reduce space debris left by post-task spacecraft and launch vehicles. It will experiment with digital simulation of space debris collisions and build a system to protect spacecraft from space debris.

In December 2008, the Key Laboratory of Space Object and Debris Observation of the Chinese Academy of Sciences was officially unveiled at the Purple Mountain Observatory (PMO) in Nanjing (Key Laboratory of Space Object and Debris Observation 2019). The laboratory set up a safety and early warning system for China in the field of space, in order to eliminate the threat posed by various human debris scattered in the vast space and protect the safety of space. The Key Laboratory of Space Object and Debris Observation will further make significant achievements in space target motion theory, space target and debris detection, spacecraft collision warning, upper atmosphere model, and so on. The laboratory will closely monitor space debris to reduce potential safety threat in space flight and detection. For the space debris discovered, the laboratory will track it in real time, search for the space garbage that has not yet been found, study the early warning technology for spacecraft launching and orbital operation, and then carry out risk assessment to resolve potential dangers.

At present, PMO has six outdoor observation stations: Qinhai Delinha Radio Observation Station, Jiangsu Xuyi Celestial Mechanics Observation Station, Jiangsu Ganyu Solar Observing Station, Heilongjiang Honghe Observation Station, Shandong Qingdao Observation Station, and Yunnan Yaoan Observation Station. Among them, Delinha Observation Station is the largest radio astronomical observation base in China. It has 13.7 m millimeter wave radio astronomical telescope, mobile submillimeter wave telescope, space debris detection optoelectronic telescope, and other large astronomical observation equipment. Xuyi Observation Station is the only celestial mechanics measurement base in China. It has the largest 1 m/1.2 m NEO detection telescope and space debris detection optoelectronic telescope in China (PMO 2019).

In June 8, 2015, the CNSA Space Debris Observation and Data Application Center was built relying on NAOC and is the technical support and daily operating organization of space debris affairs of CNSA. The establishment of the center is of great significance for promoting the development of space debris technology in China, enhancing the capacity of space debris management and service, ensuring the safety of spacecraft in orbit, supporting international space exchange and cooperation, and safeguarding the rights and interests of China's space development.

China has improved the monitoring and mitigation of early warning and protection against space debris and also enhanced standards and regulations in this regard. The monitoring of early warning against space debris has been put into regular operation, ensuring the safe operation of spacecraft in orbit. China has also made breakthroughs in protection design technologies, applying them to the protection projects of spacecraft against space debris. In addition, all Long March carrier rockets have upper stage passivation, and discarded spacecraft are moved out of orbit to protect the space environment. In the future, the standards and norms for space debris, near-Earth small objects, and space weather will be improved. In addition to this, China will establish and improve the basic database and shared data model of space debris; comprehensively promote the construction of space debris monitoring facilities, early warning, and emergency platform and network service system, strengthen the comprehensive utilization of resources; and further

strengthen the spacecraft protection capability. China will improve the space environment monitoring system, build an early warning and forecasting platform, and enhance the space environment monitoring and disaster early warning capabilities. This chapter demonstrates the construction of monitoring facilities for small near-Earth objects and the improvement of their monitoring and cataloging capabilities.

---

## **International Exchanges and Cooperation on China's Space Safety and Security**

The Chinese Government believes that international space cooperation should follow the basic principles set in the *Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interests of All States, Taking into Particular Account the Needs of Developing Countries*, adopted by the 51st United Nations General Assembly in 1996. In carrying out international space cooperation, the Chinese Government has consistently adhered to the following guiding principles:

- International space cooperation should aim at the peaceful development and utilization of space resources for the benefit of all mankind.
- International space cooperation should be carried out on the basis of equality and mutual benefit, complementarity of advantages, complementarity of strengths and weaknesses, common development and recognized principles of international law.
- The priority objective of international space cooperation is to jointly improve the space capabilities of all countries, especially developing countries, and to enjoy the benefits of space technology.
- International space cooperation should take necessary measures to protect the space environment and resources.
- Support the strengthening of the role of the United Nations Committee on Outer Space and support the United Nations Programme on Outer Space Applications.

China's international cooperation in space began in the mid-1970s. Since 2011, the Government signed 43 space cooperation agreements or memoranda of understanding with 29 countries, space agencies, and international organizations. It has taken part in relevant activities sponsored by the United Nations and other relevant international organizations, and supported international commercial cooperation in space. These measures have yielded fruitful results.

China participates in activities organized by the International Committee on Global Navigation Satellite Systems, International Space Exploration Coordination Group, Inter-Agency Space Debris Coordination Committee, Group on Earth Observations, World Meteorological Organization, and other intergovernmental international organizations. China has also developed multilateral exchanges and cooperation in satellite navigation, Earth observation and Earth science and research, disaster prevention and mitigation, deep-space exploration, space debris, and other

areas. China's BeiDou satellite navigation system has become one of the world's four core system suppliers accredited by the International Committee on Global Navigation Satellite Systems and will gradually provide regional and global navigation and positioning service as well as strengthened compatibility and interoperability with other satellite navigation systems.

The cooperation between China and Brazil on Earth Resources Satellite is smoothly progressing. On October 14, 1999, China successfully launched the first China-Brazil Earth resources satellites. In addition to the Whole-Satellite cooperation, China and Brazil have carried out a number of cooperation in satellite technology, satellite applications, and satellite components. Following the successful launch of the Sino-Brazilian Earth Resources Satellite 02 in October 2003, the Chinese and Brazilian governments signed supplementary protocols on the joint research and manufacturing of satellites 02B, 03, and 04 and on cooperation in a data application system, maintaining the continuity of data of Sino-Brazilian Earth resources satellites and expanding the application of such satellites' data regionwide and worldwide.

China and the ESA have conducted the Sino-ESA Double Star Satellite Exploration of the Earth's Space Plan. China's relevant departments and the ESA have implemented the "Dragon Program," involving cooperation in Earth observation satellites, having so far conducted 16 remote sensing application projects in the fields of agriculture, forestry, water conservancy, meteorology, oceanography, and disasters.

Furthermore, a memorandum of understanding on technological cooperation in the peaceful utilization and development of outer space was signed between China and Venezuela. The two nations have established a technology, industry, and space sub-committee under the China-Venezuela Senior Mixed Committee. Under this framework, bilateral cooperation in communications satellites, remote sensing satellites, satellite applications, and other areas is promoted. China has exported satellites and made in-orbit delivery of Venezuela's remote sensing satellite-1.

China has exported satellites and made in-orbit delivery of Nigeria's communications satellite, Bolivia's communications satellite, Laos' communications satellite-1 and Belarus' communications satellite-1.

As one of the four major GNSS providers, BDS persists in open cooperation and resource sharing, actively carries out international exchanges and cooperation, and promotes the global satellite navigation development. China has taken part in international activities organized by the United Nations and other relevant international organizations, within the framework of relevant multilateral mechanisms. Under the framework of ITU, international frequency coordination activities have been conducted. China supported the extension of the radio-determination satellite service (space-to-Earth) allocations in the S-band and successfully pushed forward the S-band as another band for navigation satellites, with joint efforts with delegates from other countries. As members of the International Committee on Global Navigation Satellite Systems (ICG) and the ICG Providers' Forum, China actively participated in the meetings held by the United Nations Committee on the Peaceful Uses of Outer Space and the seminars organized by the United Nations Office for

Outer Space Affairs. The China Satellite Navigation Conference has been held annually, with more than 3,000 attendees every year. China actively established interaction mechanisms with navigation meetings of the United States, Russia, and Europe, participated in, organized, and hosted international academic exchange activities of satellite navigation, so as to strengthen international exchanges and attract global intellectual resources to jointly promote the development of satellite navigation technologies. Under the framework of the Asia-Pacific Space Cooperation Organization (APSCO), a number of cooperative projects are being implemented in the fields of monitoring and assessment, research and applications of the BDS/GNSS compatible terminals in disaster reduction, development of BDS/GNSS software receiver, as well as education and training on satellite navigation, in order to upgrade the technologies and to strengthen fundamental capacity building of the APSCO member states.

China actively participated in activities organized by the Inter-Agency Space Debris Coordination Committee, started the Space Debris Action Plan, and strengthened international exchanges and cooperation in the field of space debris research. The nation's independently developed space debris protective design system has also been incorporated into the protection manual of the Inter-Agency Space Debris Coordination Committee.

---

## Conclusion

Currently, an increasing number of countries attaches importance to and takes part in developing space activities. Moreover, space technology is widely applied in all aspects of our daily life, exerting a major and far-reaching influence on social production and lifestyle and increasingly in the field of safety and security.

It is mankind's unremitting pursuit to peacefully explore and utilize outer space. Standing at a new historical starting line, China is determined to accelerate the pace of developing its space industry and actively carry out international space exchanges and cooperation, so that achievements in space activities will serve and improve the well-being of mankind in a wider scope, at a deeper level and with higher standards. China will promote the lofty cause of peace and development together with other countries.

---

## References

- China Centre for Resources Satellite Data and Application (2019) Retrieved 16 July 2019, from <http://www.cresda.com/EN/>
- China National Space Administration (2019) Retrieved 16 July 2019, from <http://www.cnsa.gov.cn/>
- China Satellite Navigation Office (2018) Development of the BeiDou Navigation Satellite System. Retrieved from <http://en.beidou.gov.cn/SYSTEMS/Officialdocument/201812/P020190523251292110537.pdf>
- Key Laboratory of Space Object and Debris Observation, PMO, C (2019) Retrieved 16 June 2019, from <http://www.sodo.pmo.cas.cn/>



- Land Satellite Remote Sensing Application Center (2019) Retrieved 16 July 2019, from <http://www.lasac.cn/>
- National Satellite Meteorological Center. (2019). Retrieved July 16, 2019, from <http://www.nsmc.org.cn/newsite/nsmc/channels/100003.html>
- National Satellite Oceanic Application Center (2012) National Satellite Ocean Application Service. Retrieved 16 July 2019, from [http://www.nsoas.org.cn/NSOAS\\_En/index.html](http://www.nsoas.org.cn/NSOAS_En/index.html)
- Purple Mountain Observatory (PMO) (2019) Retrieved 16 June 2019, from <http://www.pmo.ac.cn/>
- The State Council Information Office of the People's Republic of China (2000) China's space activities, A white paper
- The State Council Information Office of the People's Republic of China (2006) China's Space Activities in 2006. Beijing. Retrieved from [http://www.gov.cn/english/2006-10/12/content\\_410983.htm](http://www.gov.cn/english/2006-10/12/content_410983.htm)
- The State Council Information Office of the People's Republic of China (2011) China's Space activities in 2011. Beijing. Retrieved from [http://www.gov.cn/english/official/2011-12/29/content\\_2033200.htm](http://www.gov.cn/english/official/2011-12/29/content_2033200.htm)
- The State Council Information Office of the People's Republic of China (2015) China's military strategy. Beijing
- The State Council Information Office of the People's Republic of China (2016) China's Space Activities in 2016. Retrieved from <http://www.scio.gov.cn/wz/Document/1537091/1537091.htm>
- XINHUANET (2019) Retrieved 16 June 2019, from <http://www.xinhuanet.com/>



# Cybersecurity Space Operation Center: Countering Cyber Threats in the Space Domain

# 48

Salvador Llopis Sanchez, Robert Mazzolin, Ioannis Kechaoglou,  
Douglas Wiemer, Wim Mees, and Jean Muylaert

## Contents

Introduction .....	922
Description of the Cyber Threat Landscape Affecting Space-Based Information Systems ...	925
Electronic Warfare and Cyber Defense Convergence .....	926
Managed Cybersecurity of Space Systems Is Key .....	928
Challenges and Recommended Actions .....	929
Functional Capabilities for Implementing a Space Operation Center .....	930
Baseline Functions of a Cybersecurity Space Operations Center (CySOC) .....	930
Concept of Operations .....	933
Additional Capabilities of a Cybersecurity Space Operation Center (CySOC) .....	934
Importance of Collaborative Information Sharing and Incident Management .....	935
The Role of Education and Training for Developing a Skilled Space Workforce .....	935
Introduction .....	935
Training Environments .....	936
Designing Training Scenarios .....	937
Evaluating Training Results .....	937
Conclusions .....	938
References .....	939

---

The contents reported in the paper reflect the opinions of the authors and do not necessarily reflect the opinions of the respective agency/institutions.

---

S. Llopis Sanchez (✉)  
European Defence Agency (EDA), Brussels, Belgium  
e-mail: [info@eda.europa.eu](mailto:info@eda.europa.eu)

R. Mazzolin · I. Kechaoglou · D. Wiemer · J. Muylaert  
RHEA Group, Wavre, Belgium  
e-mail: [r.mazzolin@rheagroup.com](mailto:r.mazzolin@rheagroup.com); [i.kechaoglou@rheagroup.com](mailto:i.kechaoglou@rheagroup.com); [d.wiemer@rheagroup.com](mailto:d.wiemer@rheagroup.com); [J. Muylaert@rheagroup.com](mailto:J.Muylaert@rheagroup.com)

W. Mees  
Royal Military Academy, Brussels, Belgium  
e-mail: [wim.mees@rma.ac.be](mailto:wim.mees@rma.ac.be)

---

**Abstract**

The focus of this article is to describe the rapid changing nature of space systems where the electromagnetic spectrum and cybersecurity aspects coexist, leading to a “change of course” to ensure secure space communications. Space systems must be designed to achieve cyber resilience. Existing vulnerabilities must be mitigated as resulted from a risk management methodology. To avoid compromises of security, a security monitoring mechanism and incident response for space systems have to be implemented. The authors provide an analysis of the functional capabilities and services of a “cybersecurity space operations center.” System monitoring is essential in view of obtaining a cyber situational awareness and decision-making for space missions. Security operation center-related services could be built up in a permanent or in an ad hoc mobile infrastructure. An integrated cyber range capability to test, train, and exercise over modeled and simulated space systems will improve space operators’ skills when confronted with time-critical interventions.

---

**Introduction**

National security is not restricted to securing the land, air, and maritime boundaries and pursuing strategic interests but encompasses all aspects that have a bearing on the nation’s well-being. Outer space and cyberspace have emerged as the new enablers for nations, enhancing the speed and efficiency of national security and socioeconomic efforts and also providing novel applications in these areas. In an information-dominated world, they are instrumental in providing the competitive edge among the global community, strategic and tactical superiority in conflict situations, and projection of national power and influence. In addition to capability enhancement towards national aspirations, investments are also necessary for securing these capabilities against deliberate or unintentional intrusions or attacks and in ensuring safe and sustainable operations.

Assured access to cyberspace is a key enabler of national security. Two of the defining characteristics of a strong, modern, industrial nation are economic prosperity and a credible defense. The ability to use cyberspace has become indispensable to achieving both of these objectives. Business and finance executives, as well as senior defense leaders, rely on cyberspace for exactly the same thing – to get information, move information, and use information to make better decisions faster than the competition. The data- and information-rich environment of the modern battlespace presents a key area of both strategic opportunities and, equally, vulnerability. Both cyber and space technologies, in particular, are the new battleground for competing great powers who seek to limit opponents’ access to information, analytics, and complex surveillance and reconnaissance information with which to inform decision-making.

With growing participation, commercialization has become an integral part of space operations and is receiving active governmental support. The peaceful use of

space and the military significance of outer space continues to increase with some 60 countries currently utilizing it for peaceful purposes, for communications, banking, monitoring environmental and climate change, disaster management, e-health, e-learning and communications, and surveillance and guidance systems for military purposes. Regarding vulnerabilities, while space operations have always been vulnerable to natural forms of interference, progressive developments in the domain have also resulted in the emergence of unique novel challenges to space security and the sustainability of the environment. Greater participation in the domain and commercial prospects has more players vying for prime orbital slots, the radio frequency spectrum, and a larger share of the market. Overcrowding and increasing space debris are adversely affecting the survivability of satellites. The environment is therefore becoming more contested, congested, and competitive with the consequent increase in potential for disruption of operations. Space is being used extensively by advanced spacefaring nations for supporting military operations, and most new entrants would also leverage their access for these purposes. A corollary to this is that all assets in space providing a strategic or military advantage can be designated as valid targets in case of hostilities. Consequently, advanced nations are making efforts to dominate and control the environment to protect their interests and assured access to the realm, and the less capable ones would do the same to gain an asymmetric advantage through degradation and destruction of systems. Both these strategies demand development of counter-space threats and counter-cyber threats capabilities that would include risk mitigation actions. Such capabilities in the hands of rogue nations or non-state actors, who have limited interests in the space domain, could be extremely dangerous, even up to the catastrophic level of cascading satellite collisions. In recent years, national security challenges have necessitated a tacit acceptance of the use of the space domain for meeting national security objectives. The discussion about the creation of space forces in some countries – as a new service branch within the armed forces – to have control over military space operations is one example of the growing importance of the use of outer space.

Cyberspace is a man-made domain consisting of the interconnected networks of computing and communication devices and the information contained on these networks. Satellites and other space assets, just like other parts of the digitized critical infrastructure, are vulnerable to cyberattacks. When considering our daily lives, there is not an operation or activity conducted anywhere at any level that is not somehow dependent on space and cyberspace. This interdependency could be used to attack space assets from cyberspace. From a cyberspace perspective, it's irrelevant how high above the ground a computer is positioned. Cyber vulnerabilities associated with space-related assets therefore pose serious risks for ground-based critical infrastructure, and insecurities in the space environment will hinder economic development and increase the risks to society. Advancements in the cyber domain have not required a protracted thrust by governments towards its development as the transformational nature of the technology, its commercial potential and cheaper access, has caused a self-sustaining expansion of capabilities and capacities. Societies' increasing dependence on networks, however, has resulted in a surge in the number and sophistication of cyberattacks that exploit the hardware or software

vulnerabilities of the networks with diverse motivations and consequences. Cyber intrusions could target government agencies and departments and private corporations or individuals, with diverse impacts on national security. These could be undertaken for espionage, to commit cybercrime or for denying or disrupting critical national infrastructure systems like power grids, telecommunication networks, transportation systems, water services, or financial and banking operations. They could be used for social engineering – spreading disinformation and molding public opinion with the intention to destabilize the internal security environment of the country, as is currently being seen as part of the current western electoral dialogue, and supporting evolving hybrid warfare techniques that see aggressive state-based actors conduct provocative activities that fall slightly below the threshold to provoke political sanctions or military response. As network centrality becomes integral to military operations, military equipment and operations could be attacked to gain strategic or tactical advantage. These attacks could even be used to cause kinetic effects and acts of sabotage or to hamper national response mechanisms, all of which would endanger lives, thereby impacting the credibility of governments and the underlying societal security frameworks. More widespread and systematic attacks could escalate tensions among states.

The perpetrators of these attacks currently range from an individual to hacking syndicates that work independently or are covertly supported by governments and corporations. States as well as non-state actors could seek an asymmetric advantage by employing such attacks to undermine an adversary's security and stability. With greater technological capability, the nature and scale of cyberattacks have continued to evolve. They are now more targeted and decisive, with clear political, economic, or military motivations and intentions. The traditional lines that would have earlier helped distinguish between the types of attacks and the motivation of their perpetrators have blurred. While the state actor could resort to an attack to undermine security or stability, a similar attack could now be undertaken by non-state actors for extortion or for obtaining information that could be sold to third parties. In that sense, a cyber threat intelligence capability is paramount to prevention and preparedness.

Networks continue to expand and become more complex, and their interdependencies continue to grow, further enhancing the vulnerabilities and increasing the difficulty in providing comprehensive protection. The environment is highly dynamic, and preventive and defensive countermeasures and reactive strategies, even with continuous efforts, are finding it difficult to keep pace with the rapidly evolving threats. Cyber situational awareness and the ability to monitor the domain, identify the vulnerabilities, and detect intrusions are still not sufficiently developed. Attempts at enhancement are hampered by concerns for privacy, freedom of speech, and the free flow of information. Even as detection rates have gone up through concerted efforts, cyber forensics need to be developed for attribution, as the attacker can easily hide his tracks in this intricate, borderless cyberspace domain. International legal regimes have failed to keep pace with the rapid technological advancements in this discipline. Advanced nations, whose critical dependence on space and cyberspace exposes them to asymmetric risks of disruption, are responding to these

limitations by developing effective deterrence against misadventures, including counterthreat capabilities. Growing economies are investing heavily in computer networks and communication facilities to meet their aspirations and have received a further boost with the smartphone revolution, increasing the density and diversity of appliances used for access to the Internet. The diversity of machines makes it difficult to put in place comprehensive protection measures. Computers and networks rely mostly on foreign software and hardware, exposing them to risks associated with the global information technology supply chain. Most of the data generated in any country is exported and stored in foreign data banks using cloud computing infrastructure. Digital and smart city initiatives and the increasing involvement of the private sector in nation-building endeavors are progressive steps that are also increasing the scope and complexities of cybersecurity efforts and are further complicated by the Internet of Things (IoT). All these makes securing the domain an arduous task.

Clearly, it can be seen that most earth-based activities are touched in some manner by space when one considers the wide array of applications associated with satellite communications, precision navigation and timing, and earth and space observation. The contemporary nature of international strategic competition has reached an inflection point where national strategic security interests embrace a wide range of activities and communities ranging from traditional military to daily commercial interests. The integrity of the underlying technology base will be a central consideration to ensuring societal security and stability.

---

## **Description of the Cyber Threat Landscape Affecting Space-Based Information Systems**

Space activities have obtained an increased focus in recent years. Within the space domain, space-based information systems (for the purpose of this publication, space-based information systems – referred as space systems in the further text – can be understood as the collection of devices and networks which permit the reception, processing, exploitation, and transmission of the information having their origin or destination in any type of space mission, e.g., navigation, telecommunication, earth observation, weather monitoring, etc.) use a digital infrastructure which connects primarily ground control stations with satellites. The architecture of satellite communications is composed of a ground segment or control segment, a space segment, and a user segment. Each segment has its own information exchange requirements and protection measures. Satellites can retransmit information to other satellites using relays without the intervention of ground assets. Ground control stations are connected with other ground tracking stations to exchange information. Ground stations can deliver commands through the uplink channel to the spacecraft and can receive data via the spacecraft downlink channel.

In cyberspace – beyond the computer networks, their connections through physical cables or fiber optics – there are other communication means which are often forgotten when a threat assessment is performed: the signals. Electromagnetic

spectrum forms the invisible propagation medium through which the signals and their information flow. Electromagnetic spectrum has a remarkable influence in the space domain given the long distance between space assets and end users. The convergence between cyber defense and electromagnetic activities for space systems is even more significant. Reasons for that convergence reside in the need to keep control over space assets at any time as well as to ensure confidentiality, integrity, and availability of space operations. In the past, satellites were launched with an estimated life span of decades. Recognizing that satellites cannot be fixed easily when they are in orbit, the design of such satellites – expected to be fully operational for many years – foresaw minor and major software configuration updates to accommodate future enhancements. This contingency design might extend their estimated life cycle. In case of performing technical corrections to a satellite, stringent procedures must be put in place to prevent any disruption. The architectural design and engineering discipline of space systems are of the utmost importance. System engineering precepts for verification and validation testing (Byrne et al. 2014) expose security flaws which may not be previously identified by information security standard practices. The adopted cyber defense posture of space assets is a trade-off between a technological simplicity to permit defensible systems – which means fewer entry points known as attack vectors – and robust system architectures. Simplicity and robustness must go hand in hand, but it is not always feasible.

In this section, some cybersecurity topics relevant for space systems will be described with an expression of cyber threats and associated risks. The results will shed some light on challenges and recommended actions.

## **Electronic Warfare and Cyber Defense Convergence**

It would be difficult to understand the digital battlefield as we know it today without the information services provided by space assets, e.g., geolocation. Thanks to a global coverage, space systems enable armed forces to operate in different scenarios across the globe. Space domain is more and more a contested and congested environment where armed forces aim to preserve freedom of operation. What is at stake is the ability of a military commander to plan and conduct military operations supported by a multi-domain command and control system (multi-domain command and control system refers to an emerging doctrinal concept which proposes the use of capabilities in concert across domains, e.g., air, space, and cyber) which benefits from an integration with space systems. The global defense C4ISR (C4ISR stands for command, control, communications, computers, intelligence, surveillance, and reconnaissance) architecture leverages on space, especially because military operations are expeditionary. The armed forces are experiencing a digital transformation leading to a drastic modernization of command and control systems in all the traditional operational domains at land, sea, and air. Space systems contribute to a better integration and jointness of military operations.

The underlying physics of space communications could be altered by an adversary causing undesired events into a space mission. Space assets are equipped with thousands of sensors transmitting signals of a different nature and informing about parameters to a monitoring center. Signals may interfere with each other if they use close radio frequencies of which harmful effects depend – among other features – on the transmission power. To achieve a high level of cybersecurity in space, efforts must be pursued in promoting cyber resilience by hardening electromagnetic features of onboard space assets. Effects in cyberspace can be achieved by exploiting vulnerabilities in the electromagnetic spectrum and vice versa. Sophisticated electromagnetic techniques could make satellites vulnerable including ground equipment. Space systems must be protected against jamming or spoofing (electromagnetic jamming (United States Department of the Army 2017) is the deliberate radiation, reradiation, or reflection of electromagnetic energy, and spoofing (United States Defense Intelligence Agency 2019) is a technique that deceives a receiver by introducing a fake signal with erroneous information) and must have a capability to operate under degraded circumstances – which means to cope with limited communication capabilities.

Electronic warfare (EW) (electronic warfare (United States, Joint Publication 2012) refers to a military action involving the use of electromagnetic energy and direct energy to control the electromagnetic spectrum or to attack the enemy. EW consists of three divisions: electronic attack, electronic protection, and electronic warfare support) and cyber defense technologies need to keep pace with a fast technological development in space. Today the challenge is not to establish long-range communications that are almost taken for granted. The challenge is to secure such communications that the protocols that were born to ensure the information distribution are also valid to ensure confidentiality and resilience. Experience in this field is far from understood since the consequences of adversarial use are not publicly known. Cyber defense and EW operations are closely intertwined in a dynamic continuum like “two sides of the same coin.” Ground-based EW systems considered as counter-space capabilities must be well taken into account when assuring the survivability of space-based tactical communications. Engineering design of space systems could advocate for a redundancy of key equipment in order to maintain service continuity, notably when a cyber-electromagnetic attack occurs or could enforce the use of radio waveforms less susceptible to external interferences. An increase of cybersecurity capabilities in space will allow governments to ensure their freedom of use, despite asymmetric capabilities possessed by an adversary. The duality cyber and EW and their effects cannot be neglected when approaching security solutions for space systems.

Space is a pivotal element of defensive capabilities for the military. Intelligence, surveillance, and reconnaissance (ISR) depend largely on space as well as positioning, navigation and timing (PNT). Situational awareness in space (SSA) helps to track and collect data related to space debris which is an important matter of concern for space operations. Reported cyberattacks on space systems including their lessons learned could work backwards to structure a cyber defense posture.



## Managed Cybersecurity of Space Systems Is Key

It is impossible to fix a security vulnerability if neither monitoring nor detection capabilities are implemented into corporate networks of a given organization. This is a principle that should be obvious but pushes cybersecurity in space to become mainstream throughout all phases of space operations from the initial design, to launching and entry into service up to the final disposal phases. Like any other critical infrastructures do, space systems need to be monitored to detect malfunctioning or to correct deficiencies as they appear. But how big is this endeavor in the face of growing cyber threats affecting space systems? Can we extract some common ground to articulate a better readiness? The answers to these questions are not simple. Some ideas will follow to illustrate the complexity of the space security issues.

A few space-based cyberattacks can be found in the literature. A summary of cases grouped by the categories of the space missions affected is as follows (Zatti 2017):

- Missions on observation and exploration experienced incidents such as targeted interference and control take over.
- Missions on navigation experienced incidents such as a denial of service and spoofing.
- Missions on telecommunications experienced incidents such as deliberate jamming and unauthorized access.

Although, there are differences in the cyber threats affecting each category of space missions, a general classification can establish two main groups: (a) those focused on the *information*, e.g., infiltration in command and control networks, and (b) those targeting the space *infrastructure*, e.g., onboard components, payload, etc. The availability of cheap jamming devices has demonstrated the threat to global positioning system (GPS) applications (Cuntz et al. 2012). These threats may fall under the information category. GPS provides geolocation and timing information to a plethora of ground satellite receivers. GPS devices assist naval ships and drones to transit through international waters or to operate planned routes in the air, respectively. *GPS spoofing* (Falco 2018) has been revealed as a serious threat that could manipulate the GPS signal by injecting false data in the GPS receiver causing a miscalculation of the position – once again a clear example of the interrelated dependencies between electromagnetic signals and cyber defense. To reduce the impact of such attacks and minimize the risks, e.g., collisions at sea and deception, a backup to “classical” navigation systems could be an option besides demanding regulators to establish urgent measures, e.g., anti-jamming or anti-spoofing components or add-ons.

The commercial space sector is experiencing an explosion. The rapid emergence of low-cost *microsatellites* is characterized by a wide spreading of

commercial-off-the-shelf (COTS) products (Falco 2018). New “CubeSat constellations” could increase the satellite’s attack surface to potential hackers. Attention must be paid to ensure the adoption of minimum cybersecurity requirements before receiving an authorization to deploy in space. Policy recommendations would be focused on holding the owner of the satellite network liable for any damage that occurred and imposing a culture of “duty of care” for the space assets that private companies own, manage, operate, or develop. Another aspect of common concern which may fall under the infrastructure category is the *complex supply chains* when developing a satellite. Different suppliers may participate at various stages of the satellite’s lifecycle. This situation introduces difficulties to manage accountability of the cybersecurity measures needed to be put in place. Therefore, system integrators must be empowered to certify a cybersecurity compliance – based on security standards – of every piece of hardware and software ever installed.

## Challenges and Recommended Actions

To meet and outpace cyber threats in the space domain, it is recommended to create a cybersecurity space operations center (CySOC) as the focal point to handle cybersecurity incidents for space missions forming part of a wide area network with other security operation centers (SOC), computer emergency response teams (CERT), and security monitoring centers (SMC). CySOC is a threat-driven response with responsibilities to detect and support the mitigation of cybersecurity incidents, train space operators, and provide expertise about the convergence of cyber defense and electromagnetic activities to counter-cyber threats. An integral part of the CySOC would be a full-fledged cyber range for space systems. A cyber range would provide training, education, exercise, and testing functionalities including the promotion of a system engineering discipline aiming to build cyber resilient architectural designs of space systems avoiding architectural points of failure. Security certification and accreditation of space systems shall be governed by and construed in accordance with an overall cybersecurity certification framework.

A cyber range could simulate space scenarios including the environmental conditions present in space. Combining intelligence with cyber operations as part of the operational activity at CySOC could prevent the materialization of future attacks. An information sharing network (ISN) would allow the exchange of information of cyber threats to other space security centers. The CySOC must provide a cyber situational awareness capability for space systems contributing to a SSA. A digital forensic capability as part of an incident handling would permit to conduct forensic investigations appropriate to support attribution. An interesting concept would be the development of a mobile deployable CySOC which could complement the work of a permanent center in situations where it is necessary to conduct on-site activities, e.g., spaceports and military operations overseas.

## **Functional Capabilities for Implementing a Space Operation Center**

### **Baseline Functions of a Cybersecurity Space Operations Center (CySOC)**

The need for a cyber defense situation awareness capability (CDSA) is well documented in cybersecurity-related literature and results from extensive studies in the domain. CDSA itself is rooted in the application of foundational situation awareness (SA) concepts as applied to the cyber domain. Although there may be variants, the work of Mica Endsley (Endsley 1995a) and her decision-making model is still widely accepted as the foundation, including three levels of situation awareness (SA): perception, comprehension, and projection. Fundamental to development of any level of cyber operator SA is implementation of an appropriate means to monitor the cyber environment through collection of cybersecurity-relevant data and transforming this into information useful for the operator understanding. A CySOC provides a focal point for this essential capability of data collection and information transformation.

The CySOC focuses on the early detection of an event that may reveal an incident. It provides the necessary tools to help the analyst not only to timely classify the event but also to identify effective mitigation measures. In an effort to enhance its proactive capabilities, it will utilize any available input including a direct user input, through a call center. In addition, various threat intelligence feeds are a valuable asset to identify threats and develop mitigation measures.

Since the security analysts are not normally in control of the operational systems, the CySOC team works closely with the monitored system's administrators who implement the resulting mitigation measures. This close collaboration is also essential for continuous security protection optimization and sensor tuning to enhance the cybersecurity resilience.

As a baseline, the functional role of the CySOC is a derivation of cyber situation awareness, providing:

- (a) Knowledge and understanding of the current state of the monitored systems
- (b) Timely and accurate assessment of potential threats

Moreover, the CySOC provides incident management support and post-incident analysis capabilities to support forensic investigation of incidents. The scope of the investigation will focus on the:

- (a) Circumstances (how and why) that allowed this incident to occur
- (b) Identification of affected assets
- (c) Evaluation of the extend of the compromise
- (d) Identification of indicators of compromise (IOC)

Finally, the CySOC can produce meaningful reports containing situational awareness data, system statistics, and regulatory compliance status as deemed necessary per network/mission.

As already introduced above, the application of resulting mitigation measures is out of the scope of the cybersecurity operations. The role of the CySOC is strictly advisory to the monitored system's administrators who are responsible for the final decision and application of a mitigation strategy.

Commonly, cybersecurity operations center services are divided into the following three service packages to cover different needs of the monitored entities based on their internal cybersecurity capabilities and risk assessment:

1. **Managed Threat Detection:** The service is limited to detection and report of probable incidents,
2. **Managed Detection and Response Support:** Building upon detection and report, the service expands to incident response support in collaboration with the monitored entity.
3. **Specialized Services:** It contains additional supporting services that may be utilized on demand based on specific needs.

### **Managed Threat Detection (MTD)**

Managed threat detection service is limited to monitoring and triage of events informing the monitored entity for probable incidents that require attention. Normally it includes the following functions:

- **Call center:** In the form of a call center, utilizing telephone, email, and ticketing system, the CySOC is receiving input from the users of the monitored system as an extension to the deployed sensor. The user reports aim to enhance the capability of early incident detection covering advanced threats able to evade the monitoring infrastructure.
- **Proactive real-time monitoring and prioritization:** Aggregating and analyzing all security events from IT and operation technology (OT) systems, as well as any necessary preprocessing and visualization to provide an overview of the current situation. This encompasses immediate analysis of real-time events and data feeds such as alerts from various intrusion detection systems or other system logs. The objective is to spot probable immediate threats or incidents that require the attention of the monitored entity.
- **Reporting:** Production of meaningful reports containing system statistics and regulatory compliances status as deemed necessary per network/mission.

### **Managed Detection and Response Support (MDRS)**

The service aims to support the monitored system's incident investigation and response capabilities. The involvement of the CySOC does not stop on the reporting of a probable incident (like in MTD service) but continues with the comprehensive

investigation of the event, in collaboration with the monitored entity providing mitigation strategy advices monitoring the effectiveness of the applied measures.

Managed detection and response support will normally include the following functions:

- Incident and threat analysis: Involving the in-depth analysis of events that are categorized as an alert indicating a probable incident. This capability usually involves detailed analysis of various data artifacts from different sensors and systems.
- Situational awareness: Providing knowledge and understanding of the current state of the IT/OT systems, which can provide timely and accurate assessment of the effectiveness of the mitigation strategy.
- Incident response support and collaboration: A key capability providing the tools (both technical and administrative) to support an effective response by the monitored entity to a successful cyberattack. The CySOC will collaborate with the monitored entity in order to identify in a timely manner the most effective mitigation measures to contain and minimize the impact of a cyberattack. This involves working with affected system owners to gather further information about an incident, understand its significance, and assess the potential mission impact.
- Reporting: Expands on the MTD service reports to include development of targeted threat intelligence data for the space sector.

### **Specialized Services**

The specialized services utilize the advanced capabilities of the CySOC to support specific needs of the monitored entity. Those services can be provided on demand and may be totally independent from the other services or build upon those:

- Forensic investigation/analysis: Providing tools, means, and forensic investigation capabilities to analyze cybersecurity incidents in detail and to provide intelligence on cyberattacks in support of MDRS service or as part of post-incident analysis investigation. This encompasses analysis of digital artifacts (including various storage media, network traffic, memory analysis, etc.) to determine affected assets, identify the attack vector, produce IOCs, and establish a timeline of events.
- Threat intelligence: Ingesting institutional, governmental, or commercial threat indicators to provide timely intelligence to use against cyberattacks relevant to the monitored entity in the form of security feeds.
- Security protection optimization recommendations and system tuning: Including analysis of the monitored system's capabilities to identify required improvements, updates, upgrades, or tuning in support of the monitoring operation. This applies only to security-related devices utilized by the CySOC including, but not limited to, intrusion detection and prevention systems (IDS/IPS), firewalls, log servers, and endpoint protection solutions. The security operation team passes recommendations to the systems' owners leaving to them the implementation responsibility. The service does not provide system vulnerability assessment.

## Concept of Operations

The cybersecurity operations team is organized into three teams, called Tiers, Tier-1, Tier-2, and Tier-3, organized under a technical leader and managed by a service manager.

Tier-1 and Tier-2 analysts compose the proactive detection and analysis team. The team is responsible for identifying threats having the Tier-1 analyst to perform continuous monitoring of the alert queue (system generated or by the call center) and triaging security alerts escalating them to Tier-2 analyst for further investigation and deep-dive incident analysis. The team is also responsible for identifying mitigation measures under the supervision of the technical leader supported, when required, by the advisory team. They coordinate with the asset owners under threat for a timely and effective response providing recommendations only (no actions upon the monitored system) and situational awareness reports. In the case of MTD service, the team is limited to triage of alerts leaving the further investigation and response to the asset owners.

Real-time monitoring is dependent on the necessary presence of cybersecurity-related sensors, log collection and aggregation, event correlation, and operation of security information and event management (SIEM) tools.

Tier-3 analysts form the security advisory team. The team is composed by specialists that possess in-depth knowledge in one or more of the following fields, network security, endpoint security, threat intelligence, forensics, and malware reverse engineering, as well as the functioning of specific applications or underlying IT/OT infrastructure, acting as an incident “hunter,” not waiting for escalated incidents and closely involved in developing, tuning, and implementing threat detection analytics. Their functions include:

- Forensic investigation/analysis: In support to the forensic investigation/analysis service.
- Space threat intelligence feed production: Leveraging commercial and open threat intelligence feeds, as well as internal findings, the team produces space-specific threat intelligence. The threat intelligence results are used to improve CySOC operations (e.g., feeding the system with IOCs) and are reported to the monitored entity as part of the reporting function of MDRS service.
- Reporting: In addition to the required reports for the monitored entity, the team produces reports related to the CySOC itself. The reports include metrics on the effectiveness and efficiency of the operations, mean response time, etc.
- Monitoring system optimization: In support of the security protection, optimization recommendations, and system tuning service including also the CySOC system itself. The identified improvements for the CySOC system are implemented directly in contrast to the monitored systems in which the implementation falls under the responsibility of the system owners.
- Tool improvement and engineering (to improve effectiveness and efficiency): Encompassing improvements of existing supporting tools and engineering of new to improve the effectiveness and efficiency of the CySOC operations.

- Proactive detection and analysis team support: As subject matter experts, they support in incident response operations.

The above functions of Tier-3 analysts are aided by cyber simulation technologies. A fully functioning cyber range provides the means to analyze current and potential threats evaluating security feeds and hunting potential threats. The cyber range having the capacity to represent the monitored systems at high fidelity offers the optimal means to conduct the Tier-3 functions.

The service manager has a complete view and responsibility for the state of the service leading the daily operations. The technical leader is the senior security analyst of the proactive detection and analysis team. He has the full view of the service and the service operations status and is responsible for the coordination of CySOC operations.

### **Additional Capabilities of a Cybersecurity Space Operation Center (CySOC)**

The previous section described the baseline functions of a cybersecurity operation center. However, as previously described in this article, the realities of threats to space missions go beyond the traditional monitoring and analysis of IT/OT systems and comprise other threats including (a) those focused on the *information*, e.g., infiltration in command and control networks, and (b) those targeting the space *infrastructure*, e.g., onboard components, payload, etc. As has been described, threats against the command and control networks may include specialized threats in the electromagnetic spectrum, while threats against the onboard components may take the form of kinetic threats from other space objects.

Therefore, it is recommended that the concept of CySOC should encompass not only traditional cybersecurity operations capacity but be augmented as an all-hazards threat assessment and mitigation service as a supplemental capacity to existing space operations. While the existing roles for space operations, including signal interference detection and response or SSA, should remain as the primary operational capacity for ensuring space operations against natural or random occurrences, these operations are not designed nor equipped to assess the potential of these effects being part of a larger, intentional, threat campaign. Meanwhile, a properly equipped CySOC, having access also to signal interference analysis capabilities and SSA information, could develop a larger threat and risk-based view of SA also involving indicators of compromise (IOC) from terrestrial networks, social engineering attacks, and others.

As an added perspective, to augment the role of the CySOC towards a more complete space mission assurance capability, it is recommended that the CySOC should also analyze information from ground-based physical security surveillance systems, enabling a more complete all-hazards risk assessment capability. Certainly, in all cases, CySOC operations would remain limited to the role of analysis and response assessment, offering advisory services to space operations, network and

system operations or physical security operations, with each having their respective roles as final decision authority for implementation of the recommended mitigation response.

## **Importance of Collaborative Information Sharing and Incident Management**

It is already understood that effective cybersecurity operations have a high dependency on collaborative information sharing of cyber-relevant information. Advisory services providing reference information related to vulnerability of systems, availability of malware exploits and resulting IOCs, and threat awareness information are essential aspects of cybersecurity analysis and response assessment. However, creation of effective information sharing communities for the purpose of coordinating cyber incident response remains an elusive goal. While communities of cyber adversaries will actively collaborate to develop comprehensive attack campaigns through coordination of social engineering attack specialists, information reconnaissance and data collection, and the development of target-specific malware to penetrate systems, defenders are hampered by ineffective collaboration tools to allow secure information sharing of cyber incident information across organizational boundaries.

Fortunately, changing regulations regarding responsible disclosure, improved attitudes towards information sharing, and improved technologies to support secure and selective information sharing of cyber incident information are increasing the potential for developing a coordinated incident response capability. For example, within Europe, four pilot projects, sponsored by the European Commission, have been established to develop an EU network of cybersecurity competence centers. This initiative represents the largest ever investment into creation of a collaborative cybersecurity information sharing capacity. The current initiative includes various studies and system development activities to create secure means for partners to share information among a wide scope of trusted relationships. Instances of the proposed CySOC services should participate and collaborate among such a network of cybersecurity competence both to leverage on the derived knowledge and to contribute to improvements in cybersecurity competence. In this way, the CySOC can take advantage of knowledge coming from dependent sectors and thereby improve the effectiveness of mitigation response to threats posed to space systems.

---

## **The Role of Education and Training for Developing a Skilled Space Workforce**

### **Introduction**

Space agencies are facing the challenge to educate and train a workforce that will be required to operate in an increasingly contested and complex space environment that may be affected by deliberate adversary cyber operations (Martin and Inspector



General 2012). Space operations are moreover increasingly reliant on information system technology, and even though increasingly efforts are being dedicated to better securing networks and systems, no system of systems will ever be entirely cybersecure. Therefore, a paradigm shift is needed from information assurance to mission assurance, which has to be considered in the context of complex systems that comprise not only physical and information assets but also cognitive and social domains. Subsequently solutions need to be designed for cyber resilience with the human operator as an integral part of the solution to ensure mission control in a degraded information environment.

At this time few opportunities exist for space operators to develop a clear understanding of how cyberattacks impact the systems they manage or a space mission as a whole. When cyber events are considered in a training exercise, they are typically developed in an isolated storyline out of fear that the potential cascading effects might interfere with the other training objectives. Given the principle that you “fight like you train,” it is however essential to incorporate realistic cyber scenarios into a significant part of the education and training exercises, in order to produce a workforce that is capable of mitigating the effect of cyber incidents in an operational space system environment.

The design of cyber injects for training non-cyber operators can be performed in two possible ways (McArdle 2019). The “systems engineering approach” consists in first identifying an attack vector (weaponized file, social engineering, hardware of software supply chain, etc.) and subsequently the target of the attack (organization, mission, network, system, etc.). Next the specific effects of the identified attack opportunity are estimated, such as induced system failures, denial of service, and data exfiltration, and this effect is then simulated to the trainees.

The second approach is an “information assurance approach,” which is based on the confidentiality, integrity, and assurance (CIA) triad. By applying the loss of one or more of the CIA attributes to a specific system, the result on the broader encompassing systems of systems, on the mission or on the organization, is estimated and presented to the trainee during the training. Certain observable effects of cyberattacks may be difficult to be distinguished from more innocent technical failures; however, both situations require a different response. Therefore, it is important that trainees learn to recognize a cyberattack in order to trigger the appropriate response and recovery. This is therefore also a training objective.

## **Training Environments**

When training a space workforce, the option of training cyber incidents with live systems is not an option. This can be circumvented through the use of a high-fidelity synthetic training environment, where the operators interact with a virtual environment that runs as much as possible the real software systems combined with models and simulations of the physical phenomena the systems normally interact with. Synthetic systems exist for specific simulations or trainings. However, they are often tailored to a specific task and siloed, which makes it hard to integrate them

into a complete synthetic training environment. It is therefore necessary to encourage simulation system developers to open up their systems and to develop federation technologies to interconnect them. It is essential to be able to run multi-domain simulations, covering all ground segment systems and radio links, as well as all aspects of the space segment ranging from the power management subsystem, attitude determination and control, communications, computing and data handling, to all possible payloads (Cayirci et al. 2017). This will make it possible to design realistic scenarios that confront the trainees with their day-to-day user interfaces and with a realistic baseline system behavior.

The goal of the non-cyber workforce is not just to train them for identifying cyber incidents but also for training the interaction with the cyber workforce, so they know the procedures, the contact points, the information to provide, how not to destroy valuable forensic information, etc. Finally, the ultimate goal is to create a digital twin of the systems that the trainees are being trained for. A digital twin is a virtual representation of a system that has been loaded with the real-world inputs and environmental parameters that were acquired on the real-world system so that it can be used to accurately simulate the real-world system's behavior.

## Designing Training Scenarios

Attackers have an interest in being unpredictable. Indeed, high-threat potential actors will deliberately misrepresent their capabilities, having a stockpile of zero-day exploits at hand. They are typically capable of deploying varying tactics, techniques, and procedures (TTPs), for instance, by relying on different hacker groups. Finally, any up-to-date detailed threat intelligence covering adversaries' capabilities will likely be classified and therefore difficult to include in training scenarios. Therefore, it is impossible to design training scenarios that cover the exact incidents the trainees will face during normal operation. Nevertheless, using the available doctrinal documents from potential adversaries and drawing inspiration from documented past attacks, it will still be possible to develop relevant scenarios.

As a baseline reference for designing adversarial cyber operations, the following aspects should be considered. Adversaries will be especially interested in high-value targets, such as ground stations, communication satellites, etc. They will furthermore try to undermine trust in the information that is produced, for instance, by manipulating sensor data that is acquired by a payload or telecontrol information from the satellite itself in order to mislead the operators. Finally, they can also resort to blended strategies, where they combine kinetic attacks, like jamming or sabotage, with non-kinetic cyberattacks that reinforce and prolong the effect of the physical attack.

## Evaluating Training Results

The education and training processes will have to be periodically evaluated and improved in order to ensure that they achieve the objective of a cyber-skilled

workforce. Alongside the typical evaluation approaches for more scholarly education as well as for operational training activities, it will be necessary to ensure that the cyber-related objectives for the training have been achieved. More in particular the question that needs to be answered is whether the staff members, both in cyber and in non-cyber positions, are able to take the appropriate decisions with respect to cyber incidents and events.

A valuable approach for measuring in an objective way whether the trainees have observed and appropriately processed the necessary information to support their decisions is the situation awareness global assessment technique (SAGAT) (Endsley 1995b) that was developed by Mica Endsley and is based on her decision-making model with three levels of situation awareness (SA): perception, comprehension, and projection. SAGAT is an on-line approach for real-time, human-in-the-loop trainings that freeze the simulation at specific moments during the training and query the subjects on specific information elements situated at the three levels of SA. Unfortunately, the fact of freezing a complex training scenario does have an effect on trainee performance (Matthews et al. 2000); therefore, it may be more appropriate to use real-time probing by sending SA questions to the trainees as a part of the normal exercise communication (Jones and Endsley 2000). Since the probing should not disturb the normal operation of the trainee too much and therefore the sampling rate and size shall be limited, it may be useful to complement it with nonintrusive expert behavior observations, for instance, based on the situation awareness behaviorally anchored rating scale (SABARS) approach (Strater et al. 2001).

It must finally also be noted that cyber range-based trainings could be used for selecting operators or for verifying the required skills for candidate operators before they start a long and expensive training, in a similar way as Liu et al. did to select astronauts to be trained into qualified robotic operators (Liu et al. 2013).

---

## Conclusions

Space is changing from a selective preserve of wealthy states or well-resourced academia, into one in which market forces dominate. Current technologies bring space capability into the reach of states, international organizations, corporations, and individuals that a decade ago had no realistic ambition in this regard; and capabilities possessed a few years ago only by government security agencies are now in the commercial domain.

Space and cyber, both technologically intensive domains, need to be harnessed optimally for national security. Formulation and articulation of an all-encompassing national security policy would help define domain-specific strategies and roadmaps. There is a global trend towards increased instability in these domains as nations develop counter-space threats and counter-cyber threat capabilities. Consequently, space has been labeled as the fourth, and cyber the fifth, dimension of warfare.

The threat manifests itself in a variety of forms on a daily basis. Lacking a coherent way forward, the collective accumulation of the variety of impacts from the myriad of cyberattacks across the breadth of critical systems could serve to drain western innovation, economy, and commerce without reaching the threshold of

triggering meaningful government and military and commercial engagement and response. There has never been a more important time or imperative for us to act upon this issue given the increasing potential existential threats posed to our societies and make this a more central element of our public agenda. The potential exists for a revolution to drive space-based security.

**Disclaimer** This article is a product of the authors. It does not represent the opinions or policies of the European Defence Agency or the European Union and is designed to provide an independent position.

---

## References

- Byrne DJ, Morgan D, Tan K, Johnson B, Dorros C (2014) Cyber defense of space-based assets: verifying and validating defensive designs and implementations. *Proc Comput Sci* 28. <http://www.sciencedirect.com/science/article/pii/S1877050914001276>
- Cayirci E, Karapinar H, Ozcakir L (2017) Joint military space operations simulation as a service. In: Proceedings of the 2017 winter simulation conference. IEEE Press
- Cuntz M, Konovaltsev A, Dreher A, Meurer M (2012) Jamming and spoofing in GPS/GNSS based applications and services – threats and countermeasures. In: Aschenbruck N, Martini P, Meier M, Tölle J (eds) *Future security 2012, Communications in computer and information science*, vol 318. Springer, Berlin/Heidelberg
- Endsley MR (1995a) Toward a theory of situation awareness in dynamic systems. *Hum Factors: J Hum Factors Ergon Soc* 37(1):32–64
- Endsley MR (1995b) Measurement of situation awareness in dynamic systems. *Hum Factors* 37(1):65–84
- Falco G Job one for space force: space asset cyber security; cyber security project, Belfer Center for Science and International Affairs. Harvard Kennedy School, July 2018. <https://www.belfercenter.org/publication/job-one-space-force-space-asset-cybersecurity>
- Jones DG, Endsley MR Can real-time probes provide a valid measure of situation awareness. In: Proceedings of the human performance, situation awareness and automation: user-centered design for the new millennium, Savannah, GA (2000)
- Liu AM et al (2013) Predicting space telerobotic operator training performance from human spatial ability assessment. *Acta Astronaut* 92(1):38–47
- Martin PK, Inspector General Nasa cybersecurity: an examination of the agency's information security. US House of Representatives, Feb (2012)
- Matthews MD et al (2000) Measures of infantry situation awareness for a virtual MOUT environment. In: Proceedings of the human performance, situation awareness and automation: user centred design for the new millennium conference
- McArdle J (2019) Rethinking cyber training for the non-cyber warrior, conference summary and conclusions, Pell center for international relations and public policy. <https://pellcenter.org/wp-content/uploads/2019/01/McArdle-Rethinking-Cyber-Training-Final.pdf>
- Strater LD et al (2001) Measures of platoon leader situation awareness in virtual decision-making exercises. No. SATECH-00-17. TRW INC Fairfax VA Systems and Information Technology Group
- United States Defence Intelligence Agency, Challenges to Security in Space, January 2019
- United States Department of the Army, FM 3-12 Cyberspace and electronic warfare operations, April 2017
- United States, Joint Publication 3–13.1 electronic warfare, 8 February 2012
- Zatti S, The protection of space missions: threats and cyber threats; information and systems security. In: 3th international conference, ICISS 2017, Mumbai, India, 16–20 Dec 2017, Proceedings



# AI and Space Safety: Collision Risk Assessment

# 49

Luis Sanchez, Massimiliano Vasile, and Edmondo Minisci

## Contents

Introduction .....	942
AI and Space Safety: Collision Risk Assessment .....	944
Space Safety System .....	944
Artificial Intelligence in Engineering .....	948
Artificial Intelligence in Space Safety .....	950
Challenges for the Future .....	955
Conclusions .....	957
References .....	958

## Abstract

The New Space environment will introduce notorious changes in the space environment during the next decades with the irruption of mega-constellation, the boost of small satellites, and the generalization of low-thrust engines. Current safety strategies and collision avoidance procedures will no longer be capable to deal with the increase on conjunction alerts. Artificial intelligence appears to be the best strategy to cope with this new situation, thanks to its ability to perform faster than physical models and make decisions based on a wider range of parameters than human operators. This results in better performances when more data are available, as the situations will present on the coming years.

---

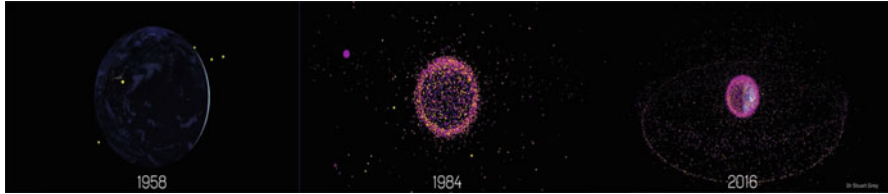
L. Sanchez (✉) · M. Vasile · E. Minisci  
University of Strathclyde, Glasgow, UK  
e-mail: [luis.sanchez-fdez-mellado@strath.ac.uk](mailto:luis.sanchez-fdez-mellado@strath.ac.uk); [massimiliano.vasile@strath.ac.uk](mailto:massimiliano.vasile@strath.ac.uk); [edmondo.minisci@strath.ac.uk](mailto:edmondo.minisci@strath.ac.uk)

## Introduction

The space environment is under a radical transformation that affects technologies, use of the space, mission concepts, and operations. Electrical propulsion, once proved its reliability and capabilities, has started to be used during the last decade on commercial and scientific satellites, both in Low Earth Orbit (LEO) and Geostationary Earth Orbit (GEO), and its use is expected to grow. In the late 1990s, technology improvements have resulted in miniaturization of space components that eventually have allowed satellites to reduce its size. Since 2003, when the first CubeSat was launched, the use of such small satellites by universities or for commercial usage has continuously increased, and it is expected to keep growing during the next decade. Along with this increase on small satellites, a higher rate of launches per year and new countries and private actors entering the scene are also expected. Among these new actors, maybe the most relevant due to its impact on the orbit environment, will be swarms and constellation mission. Along with small satellites, mega-constellations will represent the most profound change in the LEO regime during the next decade. Several of these constellations, each of them compounded by thousands of satellites, are planned and some of them have already started the deployment stage. It is expected that in the next years, the number of satellites in orbit will multiply by several times. Bearing in mind that the current number is slightly below 2,000, it will push the figures to tens of thousands of operational satellites in orbit at the same time (Lewis et al. 2017).

Space debris also increase notoriously the problem, since it is the most common type of object orbiting the Earth. Space debris refers to all man-made objects in space apart of operational satellites as well as micrometeoroids captured by the Earth's gravity. It includes upper-stage rocket bodies, inoperative satellites remaining in orbit, objects left by missions, and fragment from old satellites due to fragmentation or collision. From the beginning of the Space Era in 1958, the number of space debris objects has kept growing to reach the current state where there are in orbit more than 34,000 objects bigger than 10 cm, more than 900,000 between 1 cm and 10 cm, and millions of them even smaller (ESA Report 2019). These numbers are also expected to increase in the following years, not only linked to the increase in space traffic but also due to improvements in the current tracking techniques. New infrastructures are expected to start their operation in the next decade allowing the detection of smaller objects, which have not been possible to track until now. While this increase in the cataloged objects does not mean an increase in the actual number of objects since they are already in orbit, it will boost the number of conjunction alerts experienced by satellite operators (Haimerl and Fonder 2015) (Fig. 1).

What does it mean for safe operation of satellites? First of all, the collision of operational satellites between them or with space debris will become a more tangible threat, and the very single event of this characteristic ever happened can repeat on a more congested future space environment. In the second place, these new satellites will operate in already congested areas, some of them with limited propulsion system or with an electric one, what means more complicated and longer operations will be



**Fig. 1** Evolution of the number of objects in orbit: 1958–1984–2016. (Credits Dr. Stuart Grey)

associated to them, with an impact on the planning of collision avoidance maneuvers (CAM), more time crossing critical regions, like ISS and human space flight regions or already populated orbits. This highlights the impact of future New Space's satellites and the precariousness of the system at critical stages when agreeing a common avoidance strategy between operators, regarding that already a CAM has had to be implemented between an ESA satellite and another from Starlink mega-constellation, where this one is not even completely deployed. On the third place, the expected increase on cataloged objects can collapse the STM system, since linked to it, an increase on conjunction alerts can be expected. Despite most of these alerts does not mean a collision is going to happen or a CAM will be needed, time and effort has to be put on evaluate the risk link to each of them. If besides the probability of collision, the metric used for evaluating events as high-risk or low-risk conjunctions, presents important limitations (note that the aforementioned Iridium-33/Cosmos-2251 collision event presented a probability of collision not classified as high risk by several operators), the system leads to a catastrophic result unless major renovations are implemented (Peterson et al. 2018).

Among those renovations, automation is a major one. A shift from a system in which each satellite is operated by several agents to a system where only one operator can manage several satellites is desirable. However, such a situation is not possible with the current system structure, especially considering the expected traffic growth. It is at this point where artificial intelligence (AI) plays a crucial role. AI techniques can operate faster than current models and can take decision considering a wider set of parameters than human operators and have the capacity to perform better when the available data increases, which is the scenario expected for the next years in space. If a certain set of reliable data is provided, AI systems are able to learn directly from them and predict accurate results without the need for any physical model. In a scenario where more and more data will be available and when time is a critical resource, using the surrogate model these techniques provides can be the key for the automation of the Space Traffic Management system. While only a few examples of AI applied to Space Traffic Management can be found, they have been successfully used for predicting events, classification, and decision support in other engineering fields, including space and air traffic management. This allows thinking that AI systems are a promising trend for the next years.

The rest of the chapter deepens on the application of AI in space engineering in general, and in Space Traffic Management in particular. Beginning with, a summary

of the current situation of the Space Traffic Management (STM) and Space Situational Awareness (SSA) systems is presented, highlighting the critical situation for the future regarding the expected increase in space traffic. An overview of studies about AI in the field of traffic management, collision avoidance, and space engineering is then presented, followed by a survey of the main works on the application of AI on the STM system. Finally, some challenges to be addressed for a good implementation of AI techniques are stated.

---

## **AI and Space Safety: Collision Risk Assessment**

### **Space Safety System**

A fundamental concept in space safety is Space Traffic Management (STM), which is defined as “the set of technical and regulatory provisions for promoting safe access into outer space, operations in outer space and return from outer space to Earth free from physical or radio-frequency interference” by the IAA (International Academy of Astronautics) in the Cosmic Study on Space Traffic Management (2006, 2018). This concept includes a wide field where different knowledge areas play a role on space safety. On one hand, there are the rules, standards, and recommendations related to the satellite operations, maneuvers, conflict resolution, and collision avoidance. This group also includes the protocols to be implemented if a conjunction between two operational satellites is reported as well as the good practices on sharing satellite’s operations information. On the other hand are the technical aspects whose aim is the implementation of the previous protocols and good practices for the safe operation of the satellites, including tracking of space objects, conjunctions detection, and risk assessment as well as action for the mitigation of the risk of collision.

Another concept related to space safety is Space Situational Awareness (SSA) that involves the actions, techniques, and technologies for the tracking, orbit determination, and calculation of ephemerides of the space objects. Both SSA and STM are closed-related since the STM system needs the knowledge provided by SSA about the state of the satellites to provide conjunction alerts and perform the correct collision avoidance maneuvers (CAM) if needed. Combined, these two systems create a more complex one that involves information of thousands of space objects; requires the coordination of different operators, satellite owners, and teams; and provides alerts and recommend actions to be taken whose consequences have to be managed in a short interval of time.

Continuous monitoring of all the trackable space objects around the Earth, both operational and nonoperational satellites, is carried out by SSA service providers. The main actor is the USSTRATCOM, although commercial companies and other states are getting more relevant in the last years. When a potential encounter between one operational satellite and a piece of space debris or another operational satellite is detected when propagating the observable states, a Conjunction Data Message (CDM) is created and sent to the operators in charge on the involved satellites. Since information collected by the SSA system (USSTRACOM) presents low



quality, especially for space debris objects, the observable state and the propagated one are affected by uncertainty. A more dedicated following can be carried out to reduce this uncertainty. With all the available CDMs associated with a single event, a conjunction risk assessment is executed by the operators' CARA (conjunction assessment risk analysis) team to determine if the event represents a true threat for the satellite and the space safety or not. In the case of a high probability of collision associated with the event, a complex process starts. The first step, if the event involves two operational satellites, is agreed a common strategy, relying on manual communication between operators that delay the process. The common procedure (the two satellites moves, the biggest one moves, the one with propulsion system moves) is then analyzed with the payload team, flight dynamics team, and ground stations to come up with a possible collision avoidance maneuver strategy. This step requires a lot of coordination, time, and workload as it is critical for the success of collision avoidance. Secondly, the proposed strategy is then evaluated to ensure that the risk of the current event is reduced and no future possible collision arises: with the same object (secondary collisions) or with other bodies (tertiary collisions). Eventually, once the maneuver is approved, the event is closely monitored, and 1 or 2 days before the Time of Closest Approach (TCA), as long as the risk remains high, the CAM is performed. After the CAM is executed, the state of the satellite should be monitored again to check the maneuver has been correctly performed.

It can be seen how many critical points the performance of a single CAM associated with only one event presents. In the first place, information of conjunction is provided just a few days in advance what gives a tight interval of time for the whole process to be performed. Since CDMs are available for the last 7 days before TCA, this is the time window operators have. However, the actual time interval is shorter since first CDMs present high uncertainty and better quality data are usually required. In the second place, some of the steps involved in the process are computationally expensive and time-consuming for operators, which is added to the tight time window where the process is carry out. If better quality data are demanded for the conjunction risk assessment, sensors require time for providing accurate orbit determination information. Not only that but also accurate orbit propagation is time-consuming, and it is an operation that has to be implemented in several stages: for using actual orbits for obtaining the risk of collision, for evaluating different CAM proposals, or for assessing future collisions once the CAM is implemented. It is not just a time issue. Besides, coordination effort is a key aspect of the process. Flight control, flight dynamics, ground station team restrictions, and mission requirements have to be considered when evaluating the possible collision avoiding strategies. The coordination tasks would be even more critical if the potential collision involves two operational satellites when teams of both missions have to agree a common strategy, a problem that worsens due to the lack of protocols and specific regulations (Peterson 2019).

STM is also responsible for managing all the conjunction alerts received before the collision risk assessment process stipulates the event that represents high probability of collision or not. All those alerts that do not need a conjunction risk assessment and those that after the assessment do not require a CAM are considered

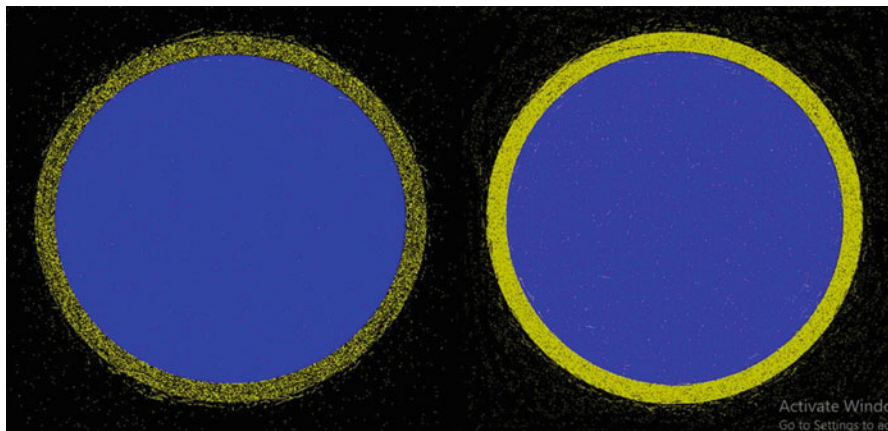
as false negatives. They do not give any information about real collisions but increase the operators' workload. There is a greater number of non-actionable alerts than actual high-risk events, which means that an important part of the resources is spent on events that are not relevant for space safety. Contrary to these false alarms (false positives), there is the possibility of false negatives to occur. False negatives are those high-risk events that are misclassified, which can lead to collision or risky events not noticed by operators in advance. As mentioned before, the collision between Iridium-33 and Cosmos-2251 was a situation like this (Peterson et al. 2018). The root of these events resides, partially, in the bad quality of initial position data, especially for the space debris objects, what makes the acquisition of better quality information essential, bringing more information to be managed by the system.

Note that the situation presented shows the current state of the system, where the traffic of space objects has not experienced the expected next year's growth. The implementation of a CAM explained above involves only a pair of space objects; however, it involves multidisciplinary teams to coordinate a lot of information in a very constrained interval of time. False alerts and false positives mentioned in the previous paragraphs currently happen. The increase on launch rate programmed for the next decade leads to the question of the scalability of the system; the final issue STM and the space safety system will face scalability. The increase on space traffic will make operators struggle in managing all the available information, and sub-optimal decisions are likely with effects on space safety. If currently, hundreds of alerts are triggered, the future space environment will push this number to limits that the system may not cope with. Since more resources should be put on filtering false alarms, the assessment of collision risk and mitigation strategies will suffer from this increase of alerts. Besides, future operators' systems would not be based on a team formed by several operators taking care of one or a few satellites, but smaller teams controlling a whole constellation with several satellites each. Such a situation is not possible unless a greater level of automatizing is implemented, and the use of a decision support system is used to replace most of the operators' tasks (Nag et al. 2018) (Fig. 2).

SSA, which is also a fundamental part of the system, also introduces critical points to the process. It is responsible for obtaining position information about all the objects orbiting the Earth, satellites, rocket bodies, or pieces of debris, as well as the ephemerides of those bodies. As can be expected due to a large number of objects orbiting the Earth, the amount of information the system has to deal with is already enormous, not counting for the expected growth of space traffic of the next decade. Furthermore, the next years will witness the start of the Space Fence system operations, the new SSA system developed by the USA for improving the monitoring of space objects. The expected increase in sensitivity will allow the track of smaller objects, invisible at the moment, including bodies in the range of 1–10 cm, making it possible to include up to 200,000 orbiting objects in the catalogs. It means that information related to space objects position and ephemerides will increase even more at a rate much bigger than the numbers of launches since most of the new objects that will enter in the catalogs are already in orbit. Another contributor to the



**Fig. 2** Operative, on deployment, and planned constellation on LEO region



**Fig. 3** Current LEO catalog versus expected catalog when Space Fence is operative

SSA system is the commercial providers that independently to the traditional sources carry out track campaigns, whose information has to be merged with those from the US and agencies' catalogs (Crosier 2016) (Fig. 3).

The New Space environment presents similarities with Air Traffic Management (ATM) and Unmanned Air Traffic Management (UTM) systems, where the increased on traffic population have forced them to adapt themselves to the new circumstances. ATM system is a well-established system which has coordinated an increasing air traffic population for several years. Key aspects of this system is the clear distribution of responsibilities, a proper set of protocols and common practices, and the effectiveness to control several objects under only one control center, which

has facilitated the automation of activities previously carried out by human operators. However, as in STM, the population growth, especially in certain regions, has forced actors involved on the system to develop a more automatic system (Kochenderfer and Chryssanthacopoulos 2011). UTM is another example where automation has been implemented to handle the rapid traffic increase and the necessity of a quick decision-making process. Some studies show the efficiency of implementing automation on the UTM and the possibility to adapt the proposed system structure to the STM (Murakami et al. 2019). Furthermore, decision support systems (DSS) based on AI has started to be implemented on unmanned aerial vehicles (UAVs) control systems not for automatizing but for supporting operators on the decision-making stage. These approaches use AI, fuzzy logic, and other related techniques for rapidly taking into account a wide set of parameters and compute a ranking of the best options to implement under a conflict, automatizing tasks previously done by operators and speeding up the whole process. Operators can then select the appropriate actions based on the ranked list of alternatives and based on certain criteria, reevaluating alternatives under new criteria or recomputing the list if more information is available. While STM presents its particularities with respect to UTM or ATM, it is clear that when traffic management systems have experienced the congestion of the environment, they have tended to the automation of the system, usually relying on AI techniques.

The successful examples of applying AI on other engineering fields, including space engineering and traffic management have boosted the interest on using these techniques on the STM system for automatizing tasks, speeding up the process, or supporting operators on taking optimal decisions in an environment that is overcoming the capacity of human operators since more and more data and variables have to be considered. Among the actors interested on implementing AI for STM, ESA and NASA can be named, both with programs to study the availability and applicability of AI methods onto real missions and scenarios (Benjamin Bastida et al. 2019; Mashiku et al. 2018). ESA has identified three main issues to be addressed by AI for facing the population increment on the orbital environment: reducing operators' workload (automation), lowering the decision-taking time on risk conjunction assessment and collision avoidance planning, and scaling down the number of false alerts.

## **Artificial Intelligence in Engineering**

Artificial intelligence is referred to as the ability of computers to learn from data and reasoning, acquire knowledge, react to the environment, and correct themselves to imitate human intelligence or behavior without being specifically programmed to do it. It is a wide knowledge area including machine learning, natural language representation, computer vision, and data mining, among many others (Russell and Norvig 2009). It has been studied for some decades, but only during the last years, with faster and more capable computers and the availability of big dataset, it has

been possible its implementation into real applications in a broad range of disciplines, including engineering (Fig. 4).

Among some of the applications of AI in engineering, one interesting field related to space safety is traffic management and collision avoidance. An important trend in recent years is the application of AI on autonomous cars. Image recognition, intelligent decision systems, and autonomous collision avoidance are issues presented in this field and addressed by AI. However, the applicability of those techniques to a completely different environment as it is space is not a straightforward task, and it is currently under research. The development of robotics has also brought some improvements in autonomous collision avoidance algorithms. Regarding the increasing autonomous of satellites, bringing them closer to the general idea of what a robot is, some attempts of extrapolating those algorithms to the space environment have been analyzed, and it is an interesting research area where promising results are expected on the next years.

The See Traffic Management (SeeTM) system presents also some examples of the application of artificial intelligence on collision avoidance. While space and maritime environment presents notorious differences, there is also some similarities, like an initial sparse and wide operational space which has experimented an increase on traffic density, having led to the necessity of implementing autonomy on the traffic management systems, or regions where this density is reaching current system limits, like ports on the see environment and the LEO region in space. In this sense, it is interesting the work presented in Statheros et al. (2008). There, an intelligent ship collision avoidance system is implemented, combining both dynamic and AI

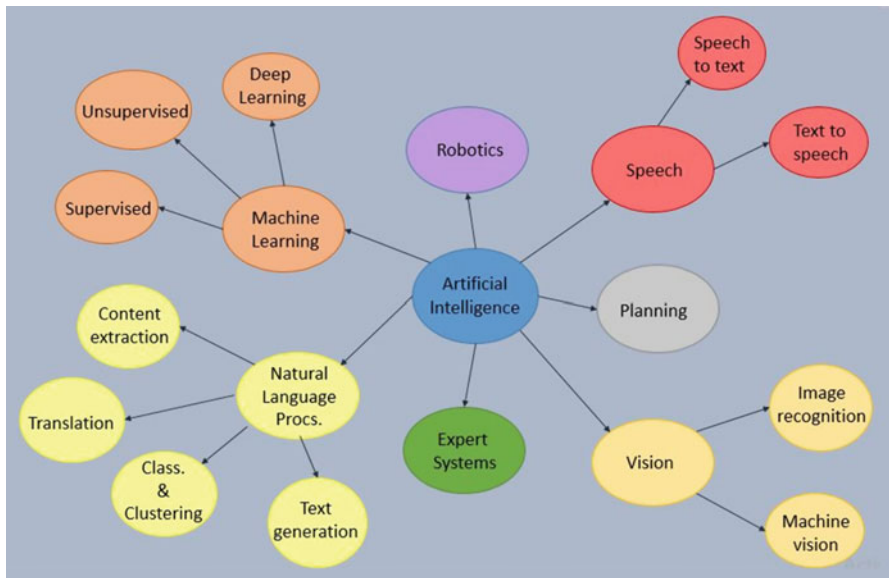


Fig. 4 Artificial intelligence areas

surrogate models. Such a system structure could be implemented, and it is on process to be implemented, on STM.

In the field of traffic management, there are also examples of using AI in the Air Traffic Management (ATM) system and Unmanned Air Traffic Management (UTM) systems. Autonomy, both on the vehicles and on the operators' activities, is spread on these systems, although not necessarily by using AI. Nevertheless, the increase in air traffic and the irruption of commercial UAVs interacting with the convectional aerial traffic have forced the system to implement AI techniques for supporting the operators on the management of the system (Kochenderfer and Chryssanthacopoulos 2011; Julian and Lopez 2016; Ramirez-Atencia et al. 2017).

The space sector is getting interested in AI too, having incorporated techniques and methods in different areas. Natural language processing (Berquand et al. 2018), knowledge representation, automated reasoning, computer vision (Jasiobedski et al. 2001), trajectory optimization and navigation (Izzo et al. 2019), satellite autonomy (Anderson et al. 2009), and robotics are some of the fields in space engineering where AI have made interesting contributions.

## Artificial Intelligence in Space Safety

It seems clear that there is a well-established field of research and application of AI in different fields of engineering, including dealing with conflict, managing traffic, and supporting decision-making. Based on the studies presented in the previous section, it is reasonable that AI and machine learning (ML) methods can be applied also in STM. As mentioned previously, space agencies and other actors involved on space safety have started to implement lines of investigation on this direction, and it is worth to explain in more detail the three main issues AI is expected to solve according to ESA (Benjamin Bastida et al. 2019):

- Reducing the tasks operators currently carry out by implementing automation. Future increase in space traffic will translate in growth on the time and effort operators will spend just dealing with alerts, classifying events, performing detail conjunction risk assessment, planning and executing maneuvers, collecting better data, or managing end-of-life strategies. Currently, some of these activities present a certain degree of automation, while others require several dedicated hours. Investing in the automation of most of these activities will allow operators to focus on the decision-making stage, on the nominal operation of satellites or the handling of more satellites simultaneously. Another important area where automatizing can liberate much of the operator's time is on the coordination between teams and other operators in the event of a conflict, switching for the current manual procedures for a much more automatic one, with clear protocols and standardized steps.
- Lowering decision-taking time. Automation of operators' tasks will allow them to spend more time and effort on the critical steps of decision-taking in collision risk assessment, collision avoidance maneuvers, or disposal strategies evaluations.

However, the expected rise in space population will imply the number of satellites to be controlled, and the amount of information to be considered will exceed human operators' capacities. AI-based systems for supporting on the decision-making stages, like DSS agents, will be able to handle all this information and propose alternative strategies to operators in much lesser time than current approaches taking into account a wider range of variables. Besides, surrogate models provided by AI techniques for skipping computational expensive propagator or dynamical models or the uses of databases with predefined maneuver examples to automatically find the optimal one are other AI-based options for reducing time in the future STM system.

- Reduce false alarms. Currently, the vast majority of conjunction alerts reported to operators correspond to events that do not require any additional action (neither avoidance maneuvers nor a more detailed evaluation). While triggering alerts, this kind of events do not imply true collision scenarios but consumes time and resources unnecessarily. In the next decade, when smaller objects can be tracked and more satellites will be in orbit, the number of such events will boost and more resources would be needed only to filter the actual collision encounters or high-risk events from all the non-actionable cases. Correctly selecting events without missing the high-risk ones (false negatives) nor wasting resources on false alerts (false positives) will be as essential as challenging for future STM, regarding current databases are dominated by those less interesting low-risk events.

While AI has been used in other areas of space engineering, its application on Space Traffic Management and Space Situational Awareness is limited. However, it is possible to find some pioneer works on this subject. While scarce, they cover different aspects of the STM and SSA system, addressing some of the previous aspects highlighted by ESA as priorities.

Some of those works are focused on improving orbit determination by the implementation of ML. In Peng and Bai (2018a), support vector machine is used for reducing the positional error of satellites after orbit determination and orbit propagation processes. In Peng and Bai (2018b), they continued with this line of research, switching from SVM to artificial neural networks (ANN). What they proposed in those works is the use of ML for improving orbital determination parting from the idea that classical models keep unused certain embedded information from historical data. Using both SVM and ANN, they tested the models for predicting a satellite's position and velocity error caused by measurement and dynamic propagation model limitations. Using the historical information of a certain resident space object (RSO) during an interval of time, they expected to find the relation between them and the aforementioned error in three circumstances: for the same RSO in the same interval of time of the historical data, but at epochs not including in the training set, for the same RSO but for times after those included on the historical data, and for near RSOs, both in the same interval as the training data and posterior epochs. They demonstrated by different numerical experiments the possibility of using ML for reducing orbit determination error and thus, improving orbit position knowledge. The benefits of this method for the SSA system are clear. While SSA is responsible

to keep track of all the thousands of RSOs orbiting the Earth, the accuracy of observations and models is restricted due to the great number of objects and limited knowledge of the environment when building the models. Being able to correct the errors associated with them, especially derived from imperfect modeling of the dynamics (drag, solar activity...) and limitations of the observation sensors will automatically provide a better position for detecting conjunctions and evaluating their risk. Nevertheless, the same authors are aware of some of the limitations affecting this approach as reported on another publication (Peng and Bai 2017). Lack of real data for propagating, time window limitations on the predictions, and restricted generalization to other objects different than the ones used for training are some of them (Fig. 5).

The previous approach corrects orbit determination and propagating errors, but it is still limited to the orbit propagation of each of the object of interest, which is time-consuming when several bodies are considered. Sanchez et al. (2019) propose an ML-based system for predicting collision encounters by using a set of ANNs for predicting the equinoctial parameters of a satellite during an interval of time, by providing exclusively the initial Keplerian parameters. By comparing the predicted orbits of a couple of objects, the equinoctial parameters obtained during the whole interval of time are good enough for estimating potential conjunctions by calculating the impact parameter (B-parameter) between the two bodies. In the end, the proposed method is not anything else but a surrogate orbit propagator that substitutes the dynamic models by a

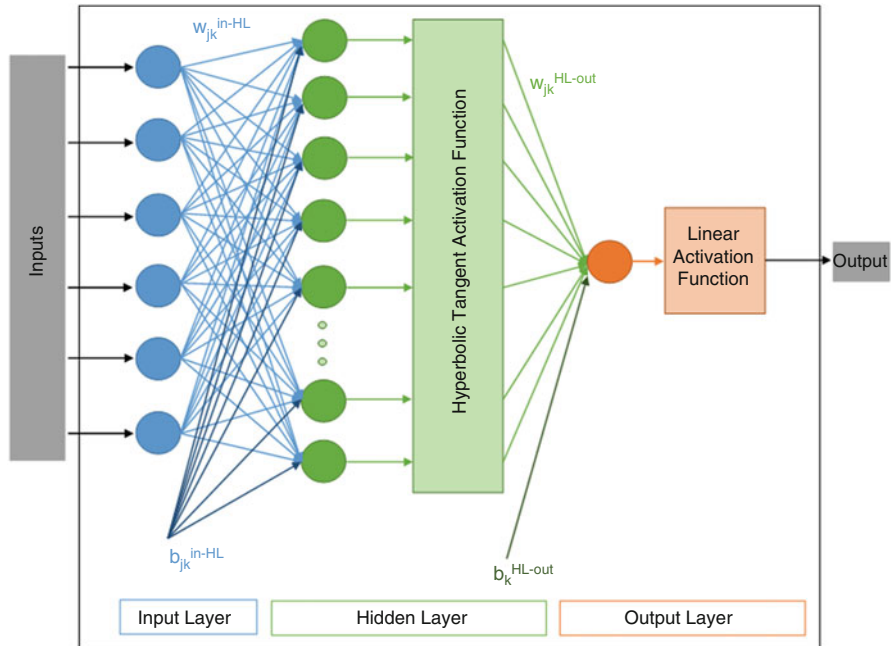
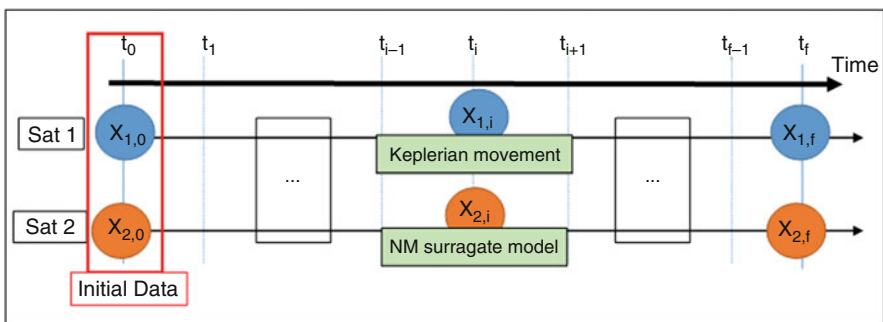


Fig. 5 ANN general structure (Sanchez et al. 2019)



surrogate model based on data. Some interesting aspects explain the importance of this approach and summarize some of the general advantages of ML. First of all, this method provides a surrogate model of the underlying problem (the two bodies perturbed movement) that does not rely on any dynamic model nor uses any integration method (nor analytical nor numerical). Since no integration is involved in the propagation, it performs faster. We are moving toward an environment where thousands of pieces can be a threat to the operational satellites and where operators will be responsible not only for one but for several of them, including constellations. Moreover, the tracking system will struggle on providing good positional data from every piece of space debris at any time. Possessing a fast and accurate model able to compute the propagate orbit of these thousands of satellites becomes crucial for the future of STM. The second advantage this approach presents is that the model relies on the data used for training. As in Peng and Bai (2018a, b), dynamic model errors are avoided since ML does not use any physical model but builds one based on the available data. In this way, by using the historical real position data, the uncertainties associated with drag, solar radiation pressure, and any other physical effects difficult to model simply do not influence the final result. As can be seen on the results proposed in Sanchez et al. (2019), the error is not dependent on the closeness to the initial epoch, as it usually happens on dynamic based orbit propagators, since an independent set of six ANN has been trained for each epoch based on the real orbital parameters of the training RSOs. This work is presented as a first step toward the use of ML in STM and, therefore, also presents some limitations: data used for training (assumed as real position) comes from a virtual database obtained by using a high fidelity propagator, and the conjunction events prediction is made assuming the Keplerian propagation of one of the satellites involved on the conjunction. However, despite these limitations and using a relatively simple ANN model, it can provide accurate results for equinoctial parameters and detection of conjunction events for RSOs different from those used during training. In addition, it performs quickly compared to orbital propagators when several object's orbits are propagated. Despite providing preliminaries results, it sets a promising path for using ML in orbit determination and orbit propagation (Fig. 6).



**Fig. 6** ANN for orbit propagation and conjunction event prediction introduced in (Sanchez et al. 2019)

Other approaches have been followed for applying AI in STM. In Sanchez et al. (2020), ML algorithms have been tested for classifying conjunction events based on a new approach for evaluating the risk assessment. The new approach pretends to overcome some limitation of a common risk assessment metric, probability of collision, by using the belief and plausibility concepts coming from evidence theory, accounting thus for epistemic uncertainty on collision risk assessment. This approach takes the conjunction geometry between two objects involved in a conjunction and includes the uncertainty from the point of view of the evidence theory. Assuming one or more sets of statistical distributions, each parameter defining those distributions is provided by the different sources (i.e., sensors or experts) as an interval or intervals, without assuming any distribution of the parameters, but only the true value is included on one of them. Each of these intervals is associated a basic probability assignment accounting for the reliability of each source, which allows taking into account aleatory and epistemic uncertainty independently. The classification criteria proposed for conjunction events are then based on the time to the encounter and belief and plausibility thresholds. Some ML methods, like artificial neural networks, random forests, support vector machine, and k-nearest neighbors, have been tested for creating two different intelligent classification systems, one using as input values of belief and plausibility as well as time and the other, considering time and geometry, allowing skipping the time-consuming step of computing the belief and plausibility curves. Each of the classes is related with an action that would be suggested to operators in the decision-making process. The results proposed in this work show the potential of using ML for supporting decision-making. Another intelligent decision support system is presented in Vasile et al. (2017). The idea of the proposed method is supporting operators in the planning and implementation of collision avoidance maneuvers when needed. An interesting contribution of this work is the creation and exploitation of a database of possible predefined maneuvers to be implemented in a conjunction event scenario. A virtual satellite position dataset was created to obtain conjunction events and later, computing the optimal maneuvers, which were stored in a new database. The new orbits generating after the CAM were also stored in the initial database and analyzed for detecting future encounters and thus, obtaining a wider range of CAMs for feeding the ML algorithms. The availability of a database with these characteristics, with a broad variety of possible maneuvers, provides fundamental information to an intelligent decision system for providing alternative proposals based on certain criteria. The criteria selected on this work considered the risk of not executing the collision compared with the risk associated with future possible collisions. The ideas presented on those works lay the foundations for future intelligent DSS for supporting operators. Other criteria can be implemented on the AI-based DSS to elaborate more sophisticated ranked lists of proposals to the operator like confidence on the sources, the inherent risk of executing a maneuver, the cost of the maneuver versus the cost of the satellite itself, restriction due to mission requirement, or fuel usage limits. Sophisticated DSS system accounting for several

variables and proposing alternatives in relative short interval if time has already proposed in other fields of traffic management (Ramirez-Atencia et al. 2017).

There is another aspect of the satellites' mission crucial for space safety: the disposal and reentry stages. The end of life of a satellite affects space safety in several aspects. First of all, it is essential for decreasing the rate of space objects in orbit, since it is the easiest way of removing bodies from space; second, during the decay stage, satellites have to cross highly populated regions, something that will become more critical when mega-constellations are completely disposed of. Finally, it is an extremely uncertain stage since atmosphere drag starts to be the dominant effect and density models are imprecise, solar activity is still not well modeled, and knowledge on the behavior of satellites during reentry is hard to predict. Minisci et al. (2017) presented a study for uncertainty propagation during the last stages of a GOCE mission. Besides the uncertainty quantification and characterization study, the use of high-dimensional model representation (HDMR) methods and the creating of large databases have set the path for the future use of AI on reentry time windows prediction. In the same work, meta-models based on AI were preliminary studied for mapping initial stated and model uncertainties to reentry time windows. Initial results suggest that it is possible to estimate the reentry window by this method and without any propagation. Further analysis is being carried out for a better implementation of this idea, and results suggest the potentiality of this approach.

Some other works and studies relating AI with space safety, STM, and SSA have been carried out recently. Furfaro et al. (2019) used recurrent neural network (RNN) and convolution neural networks (CNN) for classifying and characterizing RSOs based on their curve of light for STM. In Mashiku et al. (2019), supervised and unsupervised ML algorithms and fuzzy logic have been implemented for predicting close approaches by using not only the classical probability of collision but other parameters as well. Finally, Shabarekh et al. (2016) use ML approach for predicting where and when will maneuver be executed in the future to improve SSA capabilities.

## Challenges for the Future

AI is a promising approach for being implemented in STM to face the challenges of the new space environment expected for the next years. Space agencies, operators, and commercial agents have shown interest in these techniques to ensure the future of space satellites, and there are already ongoing researches for addressing the issues. However, being a new approach means that it has to face several challenges before we can talk about a space safety system based on AI.

As can be seen from current and past studies, a common problem is the lack of appropriate datasets for training the models. AI techniques are based on the availability of enough information to fit the models, extract information or capture the patrons relating data. However, actual information from real satellites is not always available in the desired format or with the required quality. Indeed, orbiting satellites

are periodically tracked, allowing accessing to a great amount of historical data; however, some of these objects are not tracked with good enough quality to allow AI techniques to extract reliable information or more accurate results than traditional methods. On the other hand, some information is not available at all, like maneuvers implemented by satellites, or the information is not enough to allow the AI models extracting patterns. Therefore, current AI techniques rely on simulated databases that have the advantages of creating a broad casuistic. However, an important challenge for the coming years regarding the implementation of AI is the creating of databases with information coming from real scenarios: real CDMs, information about implemented collision avoidance maneuvers, uncertainties associated with measurements, and state propagation.

Artificial intelligence involves a wide set of branches. So far, space safety has just scratched the surface on the application of those techniques in STM. Most of the methods implemented and studied are centered on the machine learning branch, more specifically on supervised learning. However, there is a wide range of possibilities in AI where STM can take techniques from. Intelligent Problem Solving, including Evolutionary Computing and Constraint Satisfaction Programming, can be an interesting branch for DSS development along with fuzzy logic, automating reasoning, or knowledge representation. Computer vision and image recognition are also open areas where STM can benefit from, besides data mining. The implementation of AI in STM is still a new research area, but the potential for solving some of the problems already identified is huge. The advantage is that AI is a more tested technology in other fields, including engineering. As has been seen, traffic management has already benefited from AI, and space engineering has already used AI techniques for some years. The current state of the art allows STM system to use these technologies and their advantages for solving its own challenges, automating tasks and speeding up processes.

There is still another challenge to face, as it is the implementation of these kinds of techniques onto real applications. The work carried out so far is focused on proving the capability of these techniques to improve the STM system and ensure space safety in the oncoming scenario. However, there is still a long way for being able to implement those techniques on real missions or in the actual system. More research has to be done for really understating the relation between training AI models and the physical laws ruling the data; more detailed studies for optimizing techniques should be performed as well as adapting the system for gradually incorporating the proven methods. It is now a perfect time for testing new approaches since the space environment is changing, and new techniques are not advisable but mandatory for the sustainability of the system, but at the same time, it is critical to implement reliable methods in order not to collapse the system. This leads to the last and main challenge the implementation of AI in STM has to face: the lack of standards on STM. Several AI-based approaches can be suggested, but as long as there are no protocols of actuation and standardized actions in conflict situations, the problem of a congested space will still be there. AI techniques as a way for supporting operators and moving to an automated scenario will work as long as a set of common rules and practices are shared by the different agents using the space.

## Conclusions

New Space will bring great challenges to space safety in the next decades. The implementation of new technologies, new concepts of satellites, and new kinds of missions, like low-thrust engines, small satellites, or mega-constellations, will push the limits of the space system to its limits. On top of all of this, the problem of space debris, which is going to become worse with the increase in space traffic, will make it completely necessary to carry out drastic changes on the system in order not to collapse it.

Although these changes can come from different approaches, there is a consensus on the space community that automation of the Space Traffic Management and Space Situational Awareness systems is one of them. To achieve the required level of automation, AI techniques arise as the most promising tool due to a series of factors. Their ability to deal with huge amount of data, and not only that but also learning from them and improving performances when more information is available, the advances on computer systems that allow its implementation both in the ground segment and in-orbit computers, the wide range of fields of application and task they can be applied to or the possibility to speed up the process where they are used, and the capacity for automation and decision-making support are just some of their advantages.

While used in other engineering fields, like traffic management or computer vision among many others, the application in space engineering started near in the past, focused on image recognition, autonomous navigation, satellite autonomy, orbit trajectories, or robotics. However, it is only in recent years where space safety has started to implement AI techniques, where only a few promising studies have been carried out. However, the trend followed by agencies and space actors points in an increasing relevance of AI for STM, and since it may be the only tool able to handle all the information the congestion environment expected for the next decade will generate.

Three main issues are expected to be addressed with the implementation of AI on space safety, space traffic management, and collision avoidance: automation of certain task to reduce operator's man workload, minimize time between decisions (conjunction risk assessment or collision avoidance planning and implementation), and reduce the number of false alerts in relation of potential high-risk conjunction events.

However, as a starting technique on the field, there are still some challenges to overcome. A common limitation already faced is the lack of proper database based on real scenarios. AI techniques are based on the availability of representative data. The creation of appropriate databases with information coming from real satellites, events, and scenarios, or at least, a database of virtual scenarios closely similar to real situations is vital for obtaining the better performance of these techniques. AI is a wide area with several fields. At this moment, only some of them have been preliminary studied, mainly focused on the machine learning area. Studying different approaches and performing analyses to determine the best AI branch to solve each problem related to space safety are highly recommendable to obtain the maximum

benefits from AI. Finally, lack of protocols and standardized practices is a drag for obtaining the best performances of some of these methods. A promising area on AI is the development of intelligent agents or intelligent decision support systems. However, these methods required a series of clear rules to provide the appropriate advice to operators. Agreeing on common rules and practices for all space actors is essential for the proper implementation of AI in space safety.

---

## References

- Anderson JL, Kurfess FJ, Puig-Suari J (2009) A framework for developing artificial intelligence for autonomous satellite operations. In: Proceedings of the IJCAI-09 workshop on artificial intelligence in space, Pasadena, 17–18 July 2009
- Benjamin Bastida V, Flohrer T, Krag, H, Merz K, Lemmens S (2019) CREAM – ESA’s proposal for collision risk estimation and automated mitigation. In: 1st international orbital debris conference, Sugar Land, 9–12 December 2019
- Berquand A, Murdaca F, Riccardi A, Soares T, Gerené S, Brauer N, Kumar K (2018) Towards an artificial intelligence based design engineering assistant for the early design of space missions. In: 68th international astronomical conference, Bremen, 2018
- Crosier C (2016) United States Strategic Command space situational awareness sharing program update. United Nations Committee on the Peaceful Uses of Outer Space, Scientific and Technical Subcommittee, 54th session, Vienna, 3 February 2016
- ESA Space Debris Office (2019) ESA’s annual environment report. Technical report, ESA. [https://www.sdo.esoc.esa.int/environment\\_report/](https://www.sdo.esoc.esa.int/environment_report/)
- Furfaro R, Linares R, Reddy V (2019) Space objects classification and characterization via deep learning and light curves: applications to space traffic management. In: Space traffic management conference, Austin, 26 February 2019
- Haimerl J, Fonder G (2015) Space fence system overview. In: Advanced Maui optical and space surveillance technologies conference proceedings, Maui, Hawaii, September 2015
- Izzo D, Märten M, Pan B. (2019) A survey on artificial intelligence trends in spacecraft guidance dynamics and control. *Astrodyne* 3, 287–299 (2019). <https://doi.org/10.1007/s42064-018-0053-6>
- Jasiobedski P, Greenspan M, Roth G (2001) Pose determination and tracking for autonomous satellite capture. In: 6th international symposium on artificial intelligence, robotics and automation in space, Montreal, June 2001
- Julian K, Lopez J (2016) Policy compression for aircraft collision avoidance systems. In: IEEE/AIAA 35th digital avionics systems conference (DASC), Sacramento, September 2016
- Kochenderfer MJ, Chryssanthacopoulos JP (2011) Robust air-borne collision avoidance through dynamic programming. Lincoln Laboratory, Massachusetts Institute of Technology, Lexington, Massachusetts
- Lewis H, Radtke J, Rossi A, Beck J, Oswald M, Anderson P, Bastida Virgili B, Krag H (2017) Sensitivity of the space debris environment to large constellations and small satellites. *J Br Interplanet Soc* 70:105–117
- Mashiku A, Frueh C, Memarsadeghi N (2018) Supervised-machine learning for intelligent collision avoidance decision-making and sensor tasking. 2018 NASA Goddard workshop on artificial intelligence, Greenbelt, Maryland, November 2018
- Mashiku A, Frueh C, Memarsadeghi N, Gizzi E, Zielinski M, Burton A (2019) Predicting satellite close approaches in the context of artificial intelligence. In: AAS/AIAA astrodynamics specialist conference, Portland, 11–15 August 2019
- Minisci E, Serra R, Vasile M, Riccardi A, Grey S, Lemmens S (2017) Uncertainty treatment in the GOCE re-entry. In: 1st IAA conference on space situational awareness, Orlando, November 2017

- Murakami D, Nag S, Lifson M, Kopardekar P (2019) Space traffic management with a NASA UAS traffic management (UTM) inspired architecture. AIAA SciTech Forum, San Diego, 7–11 January 2019. <https://doi.org/10.2514/6.2019-2004>
- Nag S, Murakami D, Lifson M, Kopardekar P (2018) System autonomy for space traffic management. In: IEEE/AIAA digital avionics and systems conference, London, September 2018
- Peng H, Bai X (2017) Limits of machine learning approach on improving orbit prediction accuracy. In: Advanced Maui optical and space surveillance technologies (AMOS) conference. Maui Economic Development Board, Wailea Marriott, September 2017
- Peng H, Bai X (2018a) Improving orbit prediction accuracy through supervised machine learning. *Adv Space Res* 61(10):2628–2646. <https://doi.org/10.1016/j.asr.2018.03.001>
- Peng H, Bai X (2018b) Artificial neural network–based machine learning approach to improve orbit prediction accuracy. *J Spacecr Rocket* 55:1248–1260. <https://doi.org/10.2514/1.A34171>
- Peterson G (2019) Establishing space traffic management standards, guidelines, and best practices. Center for Space Policy and Strategy, The Aerospace Corporation, El Segundo, California
- Peterson G, Sorge M, Ailor W (2018) Space traffic management in the age of new space. Center for Space Policy and Strategy, The Aerospace Corporation, El Segundo, California
- Ramirez-Atencia C, Bello-Orgaz G, R-Moreno MD, Camacho D (2017) Solving complex multi-UAV mission planning problems using multi-objective genetic algorithms. *Soft Comput* 21(17):4883–4900. <https://doi.org/10.1007/s00500-016-2376-7>
- Russell S, Norvig P (eds) (2009) *Artificial intelligence. A modern approach*, 3rd edn. Prentice Hall Press, Upper Saddle River
- Sanchez L, Vasile M, Minisci E (2019) AI to support decision making in collision risk assessment. Paper presented at the 70th international astronomical conference, Washington, DC, 21–25 October 2019
- Sanchez L, Vasile M, Minisci E (2020) On the use of machine learning and evidence theory to improve collision risk management. Paper presented at the 2nd IAA international conference in space situational awareness, Washington, DC, 14–16 January 2020
- Shabarekh C, Kent-Bryant J, Keselman G, Mitidis A (2016) A novel method for satellite maneuver prediction. In: Advanced Maui optical and space surveillance technologies conference, Maui, September 2016
- Statheros T, Howells G, McDonald-Maier K (2008) Autonomous ship collision avoidance navigation concepts, technologies and techniques. *J Navig* 61(1):129–142
- Vasile M, Rodriguez-Fernandez V, Serra R, Camacho D, Riccardi A (2017) Artificial intelligence in support to space traffic management. Paper presented at the 68th international astronomical conference, Adelaide, September 2017



# Space Object Behavior Quantification and Assessment for Space Security

# 50

Moriba Jah

## Contents

Introduction .....	962
Space Domain Awareness Goals: Knowing and Predicting Events and Processes .....	964
Human-Based (Soft Inputs) .....	967
Structured and Unstructured Information .....	968
Standards, Calibration, and Metadata .....	968
The Importance of “Independent Observations” and Big Data .....	969
Space Domain Information Fusion: A Model .....	970
Level 0 .....	972
Level 1 .....	973
Level 2 .....	974
Level 3 .....	974
Level 4 .....	974
Level 5 .....	975
Space Surveillance and Tracking .....	975
SSN Sensors (Taken Directly from a USSTRATCOM Fact Sheet) .....	976
Summary .....	983
References .....	984

## Abstract

As the spacefaring community is well aware, the increasingly rapid proliferation of human-made objects in space, whether active satellites or debris, threatens the safe and secure operation of spacecraft and requires that we change the way we conduct business in space. The introduction of appropriate protocols and procedures to regulate the use of space is predicated on the availability of

---

M. Jah (✉)

Department of Aerospace Engineering and Engineering Mechanics, The University of Texas at Austin, Austin, TX, USA

e-mail: [moriba@utexas.edu](mailto:moriba@utexas.edu)



quantifiable and timely information regarding the behavior of resident space objects (RSO): the basis of space domain awareness (SDA). Yet despite six decades of space operations, and a growing global dependence on the services provided by space-based platforms, the population of Earth orbiting space objects is still neither rigorously nor comprehensively quantified, and the behaviors of these objects, whether directed by human agency or governed by interaction with the space environment, are inadequately characterized.

Key goals of advanced SDA are to develop a capability to predict RSO behavior, extending SDA beyond its present paradigm of catalog maintenance and forensic analysis, and to arrive at a comprehensive physical understanding of all of the inputs that affect the motion of RSOs. Solutions to these problems require transdisciplinary engagement that combines space surveillance data with other information, including space object databases and space environmental data, to help decision-making processes predict, detect, and quantify threatening and hazardous space domain activity.

---

## Introduction

This chapter presents an introductory overview of space object behavior quantification and assessment through the lens of more known functions such as surveillance, tracking, and information fusion for space domain awareness. The presumption is that humanity as a whole will be more efficient, protected, and successful in their future space domain activities and dependencies if a common operational perspective can be achieved in the space domain. Without a common perspective of the space domain, serious operational weaknesses may result when space services and capabilities are degraded or denied to any entity by either natural or human-made causes. With the rapid assimilation of information technology globally and associated applications to the modern space domain, it becomes imperative that the world holistically maximize its total space domain awareness.

Space capabilities and services have been essential supporting utilities underpinning much of the global economy and technology for many years. However, the threats to those capabilities and services, along with the consequences of their loss or degradation, have only recently become a global concern given the proliferation of plausible threats and the growing dependence upon space throughout the world. All space capabilities and services are of individual national origin. The protection of space systems (satellites and controlling ground infrastructure) that provide the capabilities and services to users and customers is a singularly sovereign responsibility. In fact, not only the operation of those systems but the collection/acquisition and dissemination of information on and about the space domain are also inherently sovereign in nature. Since space has become more important as a contested domain extending human activity, this increasingly poses a dilemma for achieving global space security, safety, and sustainability.

Historically, two of the more pervasive challenges of integrating multi-entity-sourced data and information that contributes to space domain awareness are (a)

overcoming the national and commercial sensitivities of data sharing and (b) the accurate technical fusion of such data. Those challenges extend to the effective achievement of space domain awareness for the world. It is posited that the following three types of data and information may be more likely to be shared than other more sensitive information (e.g., space-related intelligence): (1) space surveillance and tracking, (2) space environment, and (3) radio-frequency interference experienced by space communication links. Thus, these three areas of space domain awareness are used within this chapter as the exemplars for characterizing a likely initial global space domain awareness picture.

The space domain can be defined as all conditions, areas, activities, and things terrestrially relating to space, adjacent to, within, or bordering outer space, including all space-related activities, infrastructure, people, cargo, and space-capable craft that can operate to, in, through, and from space.

Space domain awareness, in this context, can similarly be defined as the effective understanding of anything associated with the space domain that could impact the security, safety, economy, or environment of space systems or activities, globally. The definition acknowledges the supportive activities and threats related to land, maritime, air, and cyber regimes relevant to space operations. It requires the combination of space situational awareness foundations of detecting, tracking, and environmental monitoring, along with space intelligence foundations of characterizing normal behavior and sensitivity, to detecting change to know when an event or process has or is predicted to occur. A purpose of SDA is to provide decision-making processes with a timely and actionable body of evidence of behavior(s) [predicted, imminent, and/or forensic] attributable to specific space domain threats and hazards. Although there are no limits on what constitutes space domain awareness data, it is essential to initially address, at a minimum, space weather and environmental reporting, space object tracking and characterization/classification, as well as radio-frequency interference characterizations and attributions against satellite control links and communication services.

To date, SDA has lacked credible scientific and technical rigor to quantify, assess, and predict space domain threats and hazards. The current state of the art suffers from a number of inadequacies: there are no standard definitions of elements in the space domain; descriptions of space objects and events are limited; no standard method of calibrating sensors and information sources has been developed; tasking is addressed to individual sensors for specific data rather than to a more holistic system for information required to address needs and requirements; there exists no rigorous understanding of space environment effects and impacts on space objects; there is no framework that encourages and enables big data analysis and supports an investigative “from data to discovery” paradigm; we lack a consistent method to understand all of the causes and effects relating space objects and events.

The need to address these concerns has never been greater. On-orbit collisions, natural or intentional, are a global concern that threatens the long-term sustainability of our space activities and environment and worsens the impact of the space debris population growth in critical mission-dependent orbital regimes. It accounts for an increase in the useless space object population of about 1% annually (with isolated

events contributing spikes upward of 20% population growth) and jeopardizes the livelihoods of tens of millions of people who depend on critical space capabilities and services.

Traditionally, efforts to develop and maintain awareness of all trackable space objects have relied upon the USSTRATCOM's Space Surveillance Network (SSN). But these sensors are often prohibitively expensive for even the richest of nations, and the space domain is too vast for traditional space surveillance, ground- or space-based, to be truly effective by itself. Protecting important space assets, especially those that provide critical services and capabilities such as communication, weather, bank routing, position, navigation, and timing, requires a new approach encompassing twenty-first-century technology and a fundamental understanding of the processes governing the behavior of objects in space.

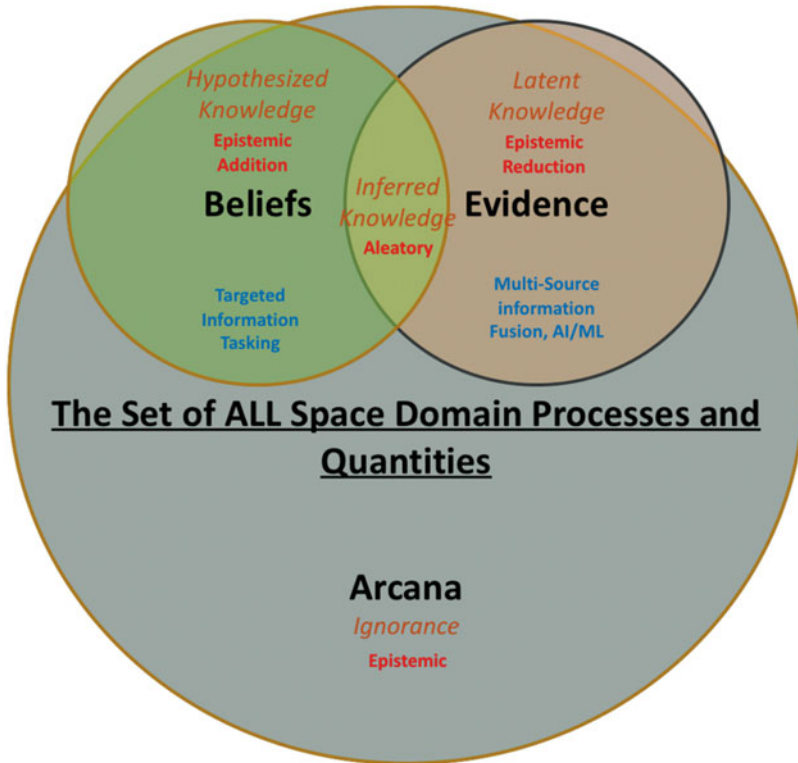
It is in this context that the following sections in this document are given and seek to place the characterization and behavior of space objects on a rigorous scientific footing. Until now, the global approach to space operations has been largely reactive, following the latest commercial exigency or governmental demand signal of the day. By contrast, the fundamental work required should lead to new ways to understand, measure, and predict behavior in space. In turn, that work will underpin the development of best practices in space traffic management and inform efforts to improve mission assurance and mitigate the effects of space debris hazards.

---

## **Space Domain Awareness Goals: Knowing and Predicting Events and Processes**

The set of all space domain events and processes, as a whole, is unknowable for many reasons. Within this whole set, we have a subset of events and processes that we believe have and are occurring. Not all of these beliefs are measured and for those that haven't been measured, we can refer to them as "hypothesized knowledge." There is also a subset of space domain events and processes that have been measured, and this is what we call evidence. However, not all evidence has been processed or used to extract knowledge. So, for evidence that has yet to be processed and either used to generate a belief or confirm or refute one, we call these "latent knowledge." Lastly, where beliefs and evidence are not mutually exclusive, we call this "inferred knowledge." The subset of space domain events and processes for which we have neither evidence nor beliefs, we acknowledge as the Arcana or "Ignorance" (Fig. 1).

Space domain awareness (SDA) is the actionable knowledge required to predict, avoid, deter, operate through, recover from, and/or attribute cause to the loss and/or degradation of space capabilities and services. The main purpose for SDA is to provide decision-making processes with a quantifiable and timely body of evidence of behavior(s) attributable to specific space threats and/or hazards. SDA encompasses all activities of information tasking, collection, fusion, exploitation, quantification, and extraction to end in credible threat and hazard identification and prediction. Understanding the synergy between the space environment, the interaction of this space environment with objects (astrodynamics), the effects of this space



**Fig. 1** Space domain events and processes

environment on objects (operational and not), and the available sensors and sources of information is critical to meaningful SDA. Included in the SDA purview is collecting raw observables, identifying physical states and parameters (e.g., orbit, attitude, size, shape), determining functional characteristics (e.g., active vs. passive, thrust capacity, payloads), inferring mission objectives (e.g., communications, weather), identifying behaviors, and predicting specific credible threats and hazards. Intuitively, SDA is a natural “big data” problem, drawing from existing and potential metadata and data sources. The problem at hand is (a) how these articulated needs can be rigorously addressed using first principles; (b) what methods, techniques, and technologies must be leveraged from other fields or targeted for development; and (c) what sensors, phenomenology, sensor tasking, or additional data are needed to support the SDA mission.

Existing research and technology focuses largely on collecting observables, identification of physical states and parameters, and determining functional characteristics. Advances include extracting observations and new information from non-traditional sensors, improving track association and initiation using admissible regions, using Finite Set Statistics methods to improve detection and tracking, and classifying space objects using ontology and taxonomy approaches.

The intent of any operational component is to predict resident space object (RSO) behavior with quantified uncertainty in order to provide decision-makers with timely warnings of specific hazards and threats. Behavior prediction must take into account the behavior of other RSOs, physics, and indirect information gleaned from non-standard sources.

To achieve this, let us focus on the foundational philosophy with which the SDA problem space should be engaged. The most important ingredient in SDA is evidence. Ideally, it all begins with that. To know something, one must measure it; to understand something, one must predict it. Both of these require observations, one to abduct knowledge and the other to demonstrate understanding. As long as one has a hypothesis that explains all past observations and can predict future ones, to within a quantifiable measure of precision, it cannot be proven that such a hypothesis is false. However, the truth about all observers is that they all lie. There is no such thing as an observer that reports the truth, because all observers (physics- and human-based) are corrupted by noise and/or bias and are of finite resolution, precision, and accuracy.

Most people attempt to force the data to answer a very specific question (i.e., estimate a specific state), yet no one has ubiquitous observations. In other words, the set of data available to the analyst is by and large almost certainly incomplete. Yet, decisions are pervasively made based upon incomplete data, and one tends to find ad hoc (and oftentimes simplifying) assumptions in place in order to arrive at such decisions. Even when the answer is obviously “insufficient information to decide,” many analysts make a decision anyway without truly understanding the consequences of deciding outside of the available information content or inferable knowledge. Another way to state this given Fig. 1 is that most decision-makers make decisions based upon hypothesized knowledge (beliefs unsubstantiated by evidence).

Robust and meaningful space domain awareness requires the analyst to embrace the complexity of the problem at hand and seek to abduct knowledge from the available data and assume nothing external to what the data allow one to assume. In other words, one must mine all of the possible and available evidence, refraining from prejudice.

I call this the “Moriba Jah Refrigerator Approach” to analysis, because it is likened to how a refrigerator cools an object. Cooling is not achieved by directly cooling the object but rather by indirectly doing so via the elimination or removal of heat from the object. Therefore, for space domain awareness, the approach should be to remove ambiguity from the system instead of attempting to estimate a sole and specifically posed state. In other words, the analyst must seek to be prejudice-free in the inference process and hypothesize as much as possible and only use the available data to discard a hypothesis that cannot explain the evidence. In so doing, all surviving hypotheses have some non-zero likelihood of being true. The analyst should make decisions based upon all the possibilities that survive the scrutiny of evidence. Not doing so exposes the end user to unquantified or erroneous risk. Imagine that in the beginning, the analyst has a body of hypotheses much like a block of marble of arbitrary shape. As data are gathered and analyzed, the analyst

must subject each hypothesis to predict what has been observed, and if a hypothesis fails to do so within acceptable and quantifiable precision, then it should be discarded and likened to chipping away pieces of marble, with the ultimate goal to reveal the statue residing within the block itself. Additionally, it would be of favor if the analyst could use data alone to form hypotheses and, in this way, not subject a priori knowledge (bias) to the analysis. This may be a role for methods such as machine learning and artificial intelligence, but these should be invoked judiciously and not in the absence of known laws of physics.

In this text, so-called hard inputs will refer to information sourced from physics-based sensors such as radars and telescopes, and so-called soft inputs will refer to information sourced from human observations or interpretations. In general, hard inputs will be numerical-valued functions, and soft inputs will be semantically valued. But this is a generality and not universally true. What follows are finer descriptions of these two sources of information.

### **Human-Based (Soft Inputs)**

Of importance to space domain awareness, which is really “decision-making knowledge” for the domain, is context. This context cannot result solely from an interpretation of physics. Although most of the tracked resident space objects (RSOs) are defunct objects, debris, there is a subset of the population that are actively controlled by humans. Moreover, humans have valuable information to provide into a system that is attempting to quantify, assess, and predict the behavior of objects in space.

Much can be learned about an upcoming launch from human-based information, such as semantic corpora like “tweets” and other online media outlets. Detecting and tracking newly launched RSOs, for example, has proven to be challenging even for the most expert space surveyors. This could be made easier if one can fuse or couple physics-based inputs (i.e., measurements from physical sensors such as radars and telescopes) with human-based inputs (e.g., an opinion or human-made observation). One example resides in the use of so-called two-line elements or TLEs. These are provided by USSTRATCOM but have no measure of precision or uncertainty associated to them. Are TLEs useful? Indeed they can be, as long as they are treated as a human-based input and not like a physical sensor measurement. Prior work by Delande et al. (2018) demonstrates how these two sources can be indeed fused to achieve improved insight into RSO trajectories. It is beyond the scope of this chapter’s section, but please refer elsewhere for more details. In essence, it is possible to model the uncertainty of a RSO driven by systematic effects or ignorance (epistemic) rather than assume all uncertainty is driven by randomness (aleatory).

One of the salient challenges in exploiting human-based information is that it must be properly curated and normalized. This can be readily understood in the following example:

Let there be an unmanned aerial vehicle (UAV) in an enclosed room with a ranging sensor in one corner but this ranging sensor is unable to detect objects in the whole room. Moreover, the room contains obstacles represented as the furniture.

Now, assume that there are also three windows allowing three humans to see into the whole room. Each human has their own microphone to provide input into the UAV guidance, navigation, and control, along with the physics-based (range) sensor. At a given moment, the UAV is on an almost assured path to colliding with a chair in the room. The range sensor can weakly observe the UAV, the first human says “watch out,” the second says “ummmmm, that’s going to hurt,” and the third says “you have an obstacle 3 meters ahead of you.” The range sensor’s input is straightforward to implement but what about the three humans? Not only do they have information that could be useful to the benefit of the UAV, but they say three very different things which all attempt to convey the same predicted event, a collision. So, these human data need to have an associate measure of uncertainty, and these semantic inputs need to be mapped to a lingua franca or “normalized” in order to minimize redundancy and confusion.

While a radar and telescope are examples of physics-based sensors, natural language processing (NLP) is an example of a human-based sensor as its objects are semantic. Finding relevant information content in a physics-based sensor can be “trying to find a needle in a haystack,” but finding relevant information content in human-based inputs can be “trying to find the needle in the needlestack.”

## **Structured and Unstructured Information**

Without spending too much time in this section, for the intents and purposes of this text, structured data are those that can be found or had in specific formats, oftentimes repeatable and defined by standards (e.g., ISO). These may be ideal in terms of how they are formatted because one can develop software and algorithms to consistently and appropriately interpret and exploit these data. However, as for unstructured data, one can think of these as serendipitous, not necessarily repeatable, or even with any metadata or ancillary information to provide more meaningful context. For example, a query “scraping” the Internet for semantic data regarding launches will result in some tweets, some online media articles, etc., and these do not have a common format or structure to them, making them more difficult to interpret. Moreover, as in the example of the UAV, many different things can be alluding to a common event or process, and this must also be inferred.

## **Standards, Calibration, and Metadata**

To several points made earlier, true and meaningful SDA cannot occur in the absence of properly engineered, modeled, and curated data. Something that makes this more straightforward to achieve is the use and adherence to standards. For space we have quite a few, such as ISO, CCSDS, RINEX, EOSSA, and others. An interpreter can be developed for each, so that when data are provided in any of them, the data can be readily “ingested” and mapped/transformed to a common and appropriately labeled framework (e.g., a graph database) that can in turn be queried

by a variety of users. If users have to interpret each type of data to achieve their space domain decision-making knowledge needs, it is impossible to have this be timely, actionable, consistent, etc. Instead, what is desired is to make this interaction with “raw” information sources transparent to the user and simply provide the user with an ability to query some form of database or knowledge graph that already contains the relevant and salient information in a way that quickly and readily provides the information required to perform analytics or other. Standards make this process simpler.

Information content can only exist in the presence of differences or rates of change. How does one know whether or not a given information source is “credible” or not? Biases are commonplace among information sources, and some are additionally noisy and corrupted by systematic or random errors. If all one has is a single clock, it is quite challenging to actually know the local time. However, if one has a time reference for comparison, one can quantify how accurate and precise one’s clock is. This underscores the importance of calibration as a frequent process within SDA. Think of information as evidence and each piece of evidence needs to be assessed for its value, relevance, and accuracy/precision. We must know how to interpret and “weigh” each source. This is the goal of calibration, and it is a critical element of meaningful data curation.

Regarding the interpretation of information from any given source, it is insufficient to simply have measurements absent context. For example, simply having several thousand observations from an unknown telescope or radar makes it almost surely impossible to exploit these data. In order for the data to be actionable, they require details regarding where they were collected, the precision of the sensor, and perhaps other information such as how they were collected or assumptions made, etc. This context or ancillary information is oftentimes referred to as “metadata.” The word “meta” means beyond. Datum is simply an assumption or premise from which inferences can be drawn. Data is the plural of datum. Hence, metadata would be “beyond the information” but really is context or information regarding the information. Metadata are critical in providing the SDA practitioner with guidance on how to use the data.

## **The Importance of “Independent Observations” and Big Data**

Related to the previous section, how does one know if one has the most accurate clock in the world? One must have access to as many clocks as possible, of all types, so that one can weigh all the independent evidence and find its “barycenter.” (Think of this term as the “center of mass” of multi-source information or evidence, when all are appropriately weighed and compared.) Then and only then can one know because then one can compare his or her clock to this information barycenter. How precise is your clock? Well, along with determining the information barycenter once can also determine how scattered or spread apart these clocks are from each other and this “variance” can provide insight on our clock’s precision. Let’s explore why independent observations are critical for SDA in an example. Let’s assume that



you have a satellite near the GEO region and have a genuine concern if any other RSO is within 1 km of your satellite. What if I told you that I predict that another RSO will be within 100 m of your satellite this time tomorrow. Would you maneuver your satellite to avoid the risk? What if I then told you that I arrived at that conclusion based upon a single sensor. Would your decision change? You might want another source (independent) of information that can either confirm or refute my hypothesis, right? In order for evidence to be the most actionable possible, it must be corroborated evidence, and this can only happen if there is at least one additional and independent source of information observing the same or common event or process. It's of little use to the global community if India makes one of their satellites explode on orbit stating that the resultant debris will all reenter the Earth's atmosphere in just over 1 month, and the United States states that they are tracking debris in higher orbits that will take decades to reenter. We have two entities with opposing hypotheses and no ability to corroborate either of these publicly. This is a global problem that must be addressed because it is only a matter of time before two entities have a dispute to resolve. What will be the body of evidence required to satisfactorily resolve the dispute?

Moreover, having lots of telescope data to observe the debris would be welcomed. Yet it is much more useful to have a lot of disparate data, so, for example, having several telescopes, radars, observers from the ground, observers from space, etc. all adding to the pool of evidence. A lot of data is just that, a lot of data. However, a lot of disparate data is so-called big data. Why are big data important? Because it provides additional perspectives and "observability" into a common event or process via mutual information that a single type of data cannot provide due to limitations in the sensor itself. No single type of sensor can observe in all wavelengths and frequencies and resolutions. Is it more powerful to see a hazard or does hearing it and perhaps even smelling it also help make a decision? Disparate sensing allows for more quickly abducting the underlying system or behavior from the data. It helps eliminate wrong answers more quickly. We should always evaluate evidence not only for its ability to support a hypothesis but perhaps even more so for its ability to discard a hypothesis.

---

## Space Domain Information Fusion: A Model

Data on the space environment and objects in it, imported into the SDA process, come from a disparate variety of sources and sensors. To maximally exploit the information, we must in some sense fuse the data. In this context, the concept of "data fusion," which is so often only vaguely defined, means that we seek quantitative answers to specific questions with the lowest uncertainty permitted by all the available data. For example, "Where will this object be next Tuesday at 3 o'clock?" or "What is the likelihood that my on-orbit network capability will be disrupted by space debris within the next 2 years?" To address this challenge, we have defined a Space Domain Information Fusion (SDIF) model, illustrated in Fig. 2.



We wish to maximize the mutual information between the evidence and our beliefs. Note that this is very different from a conventional data processing approach, which seeks to make the output (e.g., an image) “look like” the scene. A caveat is that arriving at an equivalent measure of information for soft inputs such as opinions is still a tremendous challenge.

The SDIF model is designed to demonstrate a system of systems that accomplishes a series of tasks:

- Facilitate the gathering of information from a system, driven by the specific needs of a given user.
- Autonomously determine how to weigh, trust, and process new information and evidence into the system.
- Provide a rigorous and physically and semantically consistent picture of the space domain via hard and soft input information fusion.
- Discover previously unknown elements of space objects and events via the leveraging of knowledge graphs and ontological frameworks (See <http://astria.tacc.utexas.edu/AstriaGraph>).
- Provide space object behavior and event predictive capabilities that are credibilistically quantifiable.
- Demonstrate the art of the possible in terms of decision-making processes and enabling command and control products and services.

The SDIF model provides a closed-loop information framework that can satisfy a variety of user needs, with a broad range of operational concerns, where the knowledge of the space domain is common. The framework provides a common operating picture that is consistent for all users. The model consists of six main levels as shown in Fig. 2 and described in summary as follows:

## Level 0

Here, raw (instance) data enter the system. These data sources include hard inputs from a variety of sensors and historical surveys, as well as soft inputs such as United Nations guidelines, European Union codes of conduct, country-specific doctrine and cultural beliefs, press announcements, and other open-source literature. Both are important in predicting, quantifying, and assessing space object behavior including space threats and hazards. The focus should not be constrained to information that may only seem to be relevant to the space domain, but all information, as numerous and as disparate as possible. The reason for this is that the Space Domain Information Fusion model, coupled to the exploitation of knowledge graphs and ontologies, will see to discover things regarding the behavior of space objects and events via correlations with any seemingly unrelated information. For instance, what if there is movement of certain space objects prior to each G7 summit? One would never know this unless these events could be easily linked and correlated. The following are examples of information sources:

- Information relevant to space object operational status
  - Owner/operator telemetry
- Information relevant to space object and event behavior and dynamic models
  - Thruster activity
  - Thermal profile (radiation and energy balance)
  - Solar/Earth radiation and Earth albedo
  - Outgassing
- Information relevant to non-dynamic models
  - Sensor performance (noise, biases, and latencies)
  - Sensor locations and Earth orientation parameters (EOPs)
  - Media corrections (atmospheric refraction, signal delays, etc.)
- Space object and event background, context, and sensor/metadata
  - JSpOC or country mission catalogs: TLEs, VCMs, state vectors, conjunction assessments
  - Observations from ground- or space-based sensors
  - Commercial data providers (e.g., AGI, GMV, ISON, Airbus, Zodiac Systems)
- Space object and event historical and country-specific behavior
  - Known break-up events
  - Known anti-satellite (ASAT) weapon tests
- World history, news, and geopolitical information
  - Councils, summits, wars/armed conflicts, etc.
  - Financial trends, events, etc.

## Level 1

This forms the heart of the system: it is the foundational piece that must be correct. The space domain is described through knowledge graphs with relationships between objects described by a set of ontologies (schema). A behavioral database, models of the physics, and other information about the space domain “universe” are at this level. This is where all incoming information and evidence is stored, before and after processing, and where past, current, and predicted knowledge and beliefs about our “logosphere” reside. The fundamental function of this level is to go “from data to discovery”: it is designed to leverage big data science and analytic methods. Whenever anyone wants to know something regarding space objects and events, this is where that information will be drawn from and, if absent, will generate an information request that will be sought to be achieved. This graph-based database also contains and maintains various representations of uncertainty and ambiguity associated with the data. At this level, no judgements are made regarding the behavior of space objects and events. Here are examples of categories and mechanisms of information to be stored and managed:

- Knowledge graphs and ontologies
  - Consistent and rich representation of space objects and events that facilitates linking of large and disparate sources of information

- Behavioral context and history
  - Cultural/societal perspectives
  - Known past behavior and events
  - Geopolitical positions
- Physics-based models
  - Space environment
  - Space objects
  - Astrodynamics
  - Sensor and information systems
- Information storage and management
  - Dynamic nature
  - Concurrent access and sharing

## Level 2

This is where our beliefs and knowledge in Level 1 are subjected to critical scrutiny. Here also we assess the degree to which any new evidence can be trusted and, if the evidence indicates that our beliefs should change, to what extent we allow that change to be made or our confidence in our belief to be adjusted. What do we do when evidence seems to conflict each other? How do we quantify, incorporate, and fuse the information we might find in someone's opinion? So far, no specific questions have been asked of the information; the intent is simply to update knowledge of the "logosphere" as described to the extent possible given the evidence provided. No judgments are made.

Once our beliefs have been rectified (confirmed, changed, or neither because any new evidence was unrelated), any changes are mapped back to Level 1 to bring our knowledge up to date.

## Level 3

Here is where we ask specific questions about things in our "logosphere" and where the tools of our analyses are brought to bear to make judgments about those things and their relationships. Users will supply their own questions and decision-making criteria. For example, to one user an object 1 km from a specific space asset may be threatening. Another may be comfortable with a separation as small as 100 m. Level 3 takes the knowledge from Level 1 and assesses it against user-defined criteria.

By keeping Levels 2 and 3 separate from Level 1, users can apply different evidence and judgments to the information without changing how space objects are defined and represented. In this paradigm, the picture of the space domain is consistent regardless of the specific user.

## Level 4

At Level 4, decisions are made by addressing questions such as "Should I do something?", "If I do this, what is the expected effect?", and "What other

information do I need to decide between these three courses of action?" Some courses of action might be predetermined by the user, and others not. The user may simply be looking for a body of evidence of something occurring in the space domain that concerns them.

A not-so-subtle issue at this level is the notion of confidence. If the user is concerned with having any other space object within 1 km of their own, how accurately must we know the answer? If our answer were "object X will be within 1 kilometer of object Y tomorrow at noon UCT," the customer will ask "what's the error on that?" If our reply is "+/- 10 kilometers," the customer may likely choose to do nothing because the level of uncertainty may not warrant the effort and risk. Thus, it is critical to have not only the customer's criteria for warning or notification but also the level of knowledge required to enable a decision. This is part of what is meant by providing "actionable" knowledge. There is work that aims to quantify this measure of confidence regardless of whether from hard or soft inputs (Bever et al. 2019).

## Level 5

Any output from Level 4 that leads to a requirement for further information passes to Level 5 where sensors and information sources are tasked to collect new information. Other non-information gathering actions may also be tasked. A prioritized list of actions is established and executed. The user has a lot of flexibility into what happens at this level.

---

## Space Surveillance and Tracking

As defined by the United States Strategic Command (USSTRATCOM), space surveillance involves (but is not limited to) detecting, tracking, cataloging, and identifying man-made objects orbiting Earth, which include active/inactive satellites, spent rocket bodies, debris, and fragments. Space surveillance accomplishes the following:

- Analyze new space launches and evaluate orbital insertion.
- Detect new man-made objects in space.
- Chart present position of space objects and plot their anticipated orbital paths.
- Produce and maintain current orbital data of man-made space objects in a space catalog.
- Inform NASA and other government entities if objects may interfere with the orbits of the Space Shuttle, the International Space Station, and operational satellite platforms.
- Predict when and where a decaying space object will reenter the Earth's atmosphere.

- Prevent a returning space object, which to radar looks like a missile, from triggering a false alarm in missile-attack warning sensors of the United States and other countries.
- Determine which country owns a reentering space object.
- Predict surface impacts of reentering objects and notify the Federal Emergency Management Agency and Public Safety Canada if an object may make landfall in North America or Hawaii.

It is important to note that USSTRATCOM developed and implemented this process and sensor network since the launch of Sputnik. As such it has been improved in an evolutionary process and does not represent the art of the possible in terms of space surveillance capability. If one were to develop a space surveillance and tracking network and system at present, it would probably not look (or operate) like the USSTRATCOM Space Surveillance Network (SSN).

### **SSN Sensors (Taken Directly from a USSTRATCOM Fact Sheet)**

The SSN uses a series of sensors to achieve its mission. Below is a brief description of each type of sensor:

**Phased-array radars** can maintain tracks on multiple satellites simultaneously and scan large areas of space in a fraction of a second. These radars have no moving mechanical parts to limit the speed of the radar scan – the radar energy is steered electronically. A detection antenna transmits radar energy into space in the shape of a large fan. When a satellite intersects the fan, energy is reflected back to the detection antenna, where the location of the satellite is computed. Two examples of these radars include Cavalier AFS in North Dakota and Eglin AFB in Florida.

**Conventional radars** use moveable tracking antennas or fixed detection and tracking antennas. A tracking antenna steers a narrow beam of energy toward a satellite and uses the returned energy to compute the location of the satellite and to follow the satellite's motion to collect more data. These radars include the Altair complex at the Reagan Test Site in the Kwajalein Atoll and the Haystack Millstone facility at the Massachusetts Institute of Technology.

**Electro-optical sensors** consist of telescopes linked to video cameras and computers. The video cameras feed their space pictures into a nearby computer that drives a display scope. The image is transposed into electrical impulses and recorded on magnetic tape. This is the same process used by video cameras. Thus, the image can be recorded and analyzed in real time.

**Midcourse Space Experiment (MSX)** satellite is a low-Earth orbiting satellite system with a payload containing a variety of sensors, from UV to very-long-wave IR. Originally a platform for Ballistic Missile Defense Organization (now known as the Missile Defense Agency), the MSX was moved to the SSN in 1998.

**Ground-based electro-optical deep space surveillance** sites assigned to Air Force Space Command (AFSPC) play a vital role in tracking deep space objects.

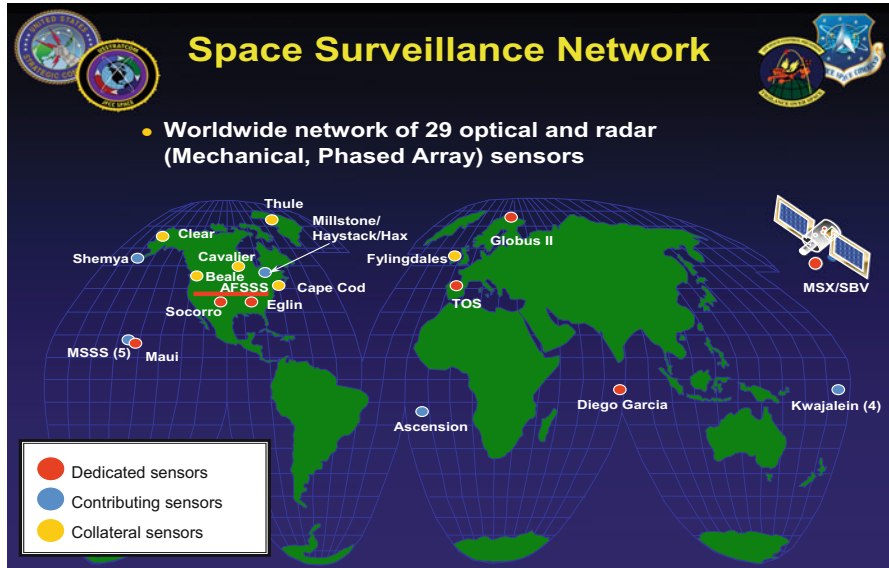


Fig. 3 Space surveillance network

Between 2000 and 2500 objects, including geostationary communications satellites, are in deep space orbits more than 22,500 miles from Earth.

The SSN sensors are categorized as dedicated (those with the primary mission of performing space surveillance) or contributing and collateral sensors (those with a primary mission other than space surveillance). Combined, these types of sensors take between 300,000 and 400,000 observations each day (Fig. 3).

### Space Object Tracking

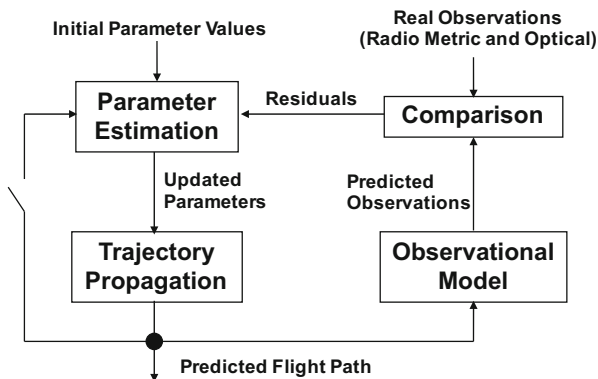
Without loss of generality, tracking an individual in a population implies an ability to “tag” (read uniquely identify) the individual and monitor this individual through time/space/frequency with quantifiable ambiguity or uncertainty, evaluating the interaction of the individual with others and its environment. However, if an individual cannot be physically tagged (or labeled) in a uniquely identifiable way, this poses serious limitations and challenges to space surveillance and tracking, which is indeed the case we face.

Tracking a space object means that one can identify this object with quantifiable and acceptable ambiguity and reconstruct and predict its behavior (usually referring to its location or motion). When this is constrained to the object’s trajectory or flight path, this process is more commonly known as orbit determination and prediction as shown schematically in Fig. 4.

Orbit determination (OD) is the process of adjusting trajectory models to best match the observed tracking data and quantify the error associated with the trajectory estimated. The collected tracking data are the actual or *Observed* measurements. The



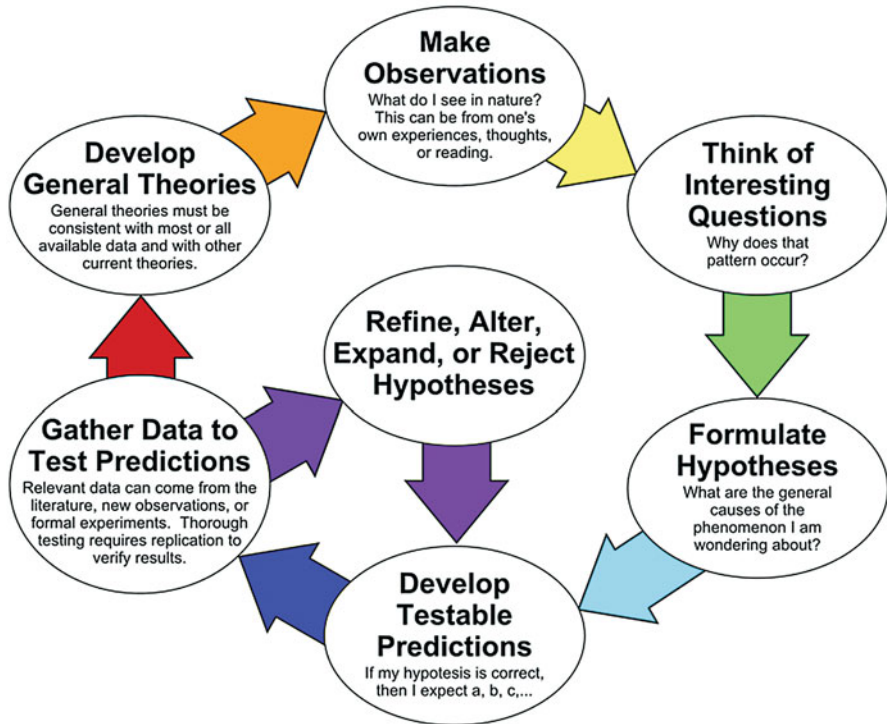
**Fig. 4** Orbit determination process



trajectory models produce predicted or *Computed* measurements. Then, what are termed *Data Residuals = Observed–Computed* measurements. The OD method typically aims to minimize the residuals by adjusting the trajectory models. These residuals are minimized in a weighted least-squares sense. The OD process accounts for measurement accuracies and accuracies with which parameters were known before taking measurements (a priori *uncertainty*). The OD produces (a) an updated trajectory estimate and (b) an estimate of error associated with current trajectory prediction. The various forces influencing the motion of the space object must be understood. An example list of these forces follows:

- Gravitational forces
  - Dominant body force (dominant body is treated as spherically symmetric; produces pure Keplerian motion)
  - Non-dominant body forces (third body forces)
  - Dominant body gravity field asymmetries
  - General relativistic effects
- Non-gravitational forces
  - Thruster activity
    - Trajectory correction maneuvers or orbit trim maneuvers
    - Attitude control system
    - Angular momentum desaturations (AMDs)
  - Solar radiation pressure and Earth albedo/radiation
  - Thermal radiation
  - Aerodynamic effects (Drag)
  - Gas leaks (real or compensative)
    - Propulsion system
    - Outgassing
    - Unknown/unmodeled accelerations

OD, especially for uncooperative space objects, requires scientific detective work. Applying the scientific method as an ongoing process is what successful



Graphic By ArchonMagnus - Own work, CC BY-SA 4.0, <https://commons.wikimedia.org/w/index.php?curid=42164616>

**Fig. 5** Scientific method as an ongoing process

OD requires (refer to Fig. 5). The OD process is subjective in that the result is not unique given a variety of assumptions on the space environment models, the astrodynamics models, and the sensor or observation system models. Moreover, the result will also differ depending on what states and parameters are estimated and the assumed prior uncertainty on these. There is a finite amount of information contained within any given set of data, and the resulting state estimate greatly depends upon what is asked of the data.

Determining a space object's orbit is typically much easier than predicting it. In order to best predict a trajectory, the OD process must attempt to not only reconstruct the trajectory of the space objects but also infer or refine knowledge of key model parameters, dynamic and non-dynamic. The only way to demonstrate that one truly understands the space object's behavior and its interaction with the space environment is via the ability to accurately predict its behavior as corroborated by future observations.

Trajectory prediction involves accurately modeling and estimating all past forces and events, as well as predicting all forces and future events. This includes the

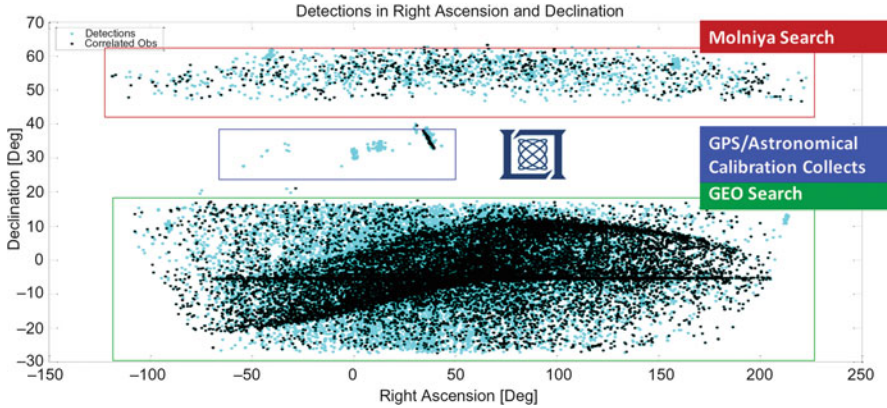
current *Estimated* trajectory error, as well as all future, or non-estimated errors that can also contribute (*Considered* error sources). More specifically, there is a need to consider the error contribution due to any uncertainty in model parameters that cannot be estimated in the OD solution. For maneuvering space objects, future thrusting events are uncertain (even if predicted) and must be included as potential uncertainties that cannot be estimated (i.e., there is a random error in every thrusting event). Many times the orientation, size, and material properties of the space object are unknown, and their uncertainty should be considered upon the influence and uncertainty in the predicted trajectory as well.

OD cannot be absolutely validated because the collected data do not have *observability* into all components of state. There are several indicators of solution quality: Regarding quality of fit, are the data residuals mean zero with no systematic trends? Regarding estimated parameters, are estimates realistic, within a priori uncertainties? The solution quality can be trended by comparing various solution strategies that are (a) data span dependent, (b) data type dependent, (c) sensor dependent, and (d) model assumptions dependent.

One of the most challenging tasks in space surveillance is in associating detections to unique objects. Many studies and analyses regarding space surveillance make two fundamentally flawed assumptions: (1) if the space object is in the sensor field of view, it is detected with a probability of one; (2) if a space object is detected, it is known which space object generated the detection. The problem with the first assumption is that the probability of detection is never exactly one; several things contribute to the total probability of detection. The probability of detection is comprised of three components: (1) a sensor-dependent component, (2) a dependence on everything between the sensor and the object, and (3) an object-dependent component. Rarely, if ever, are all three components known with absolute certainty. The problem with the second assumption is that there is always some level of ambiguity in the detection-to-object assignment unless the object is transmitting/transponding a known frequency.

This was the challenge raised earlier in the context of being able to uniquely tag and track individuals in the population. To highlight the extent of this issue, please refer to Fig. 6 which shows a plot of detections made in a single night by the Space Surveillance Telescope (SST) located near Socorro, New Mexico. Every dot is a detection generated by a space object in various orbital regimes: Molniya (highly eccentric orbits or HEO), Mid Earth Orbit (MEO) with Global Navigation Satellite Systems (GPS, etc.), and the near geosynchronous regime (GEO). All of the dots that are black are detections that were associated/correlated to unique known objects. All of the other dots are detections generated by space objects that are unknown. At least 50% of all detections are generated by unknown (read untracked) objects. This is a major unresolved issue.

In essence, the problem is as follows: given a series of observations (tracking data), determine which detections belong to unique objects and compute their trajectories. One mechanism for performing this is via Joint Probabilistic Data Association (JPDA) (Stauch et al. 2017). A simpler approach is nearest neighbor (NN) which is somewhat captured in the schematic that follows, but this simpler



**Fig. 6** Correlated versus uncorrelated detections from the Space Surveillance Telescope (SST)

approach tends to suffer from higher false positives (i.e., associating data from objects that are not the same, assuming a unique object).

Figure 7 shows a series of unassociated detections at an initial time, and then a set of hypotheses are computed from these. These hypotheses are compared to future data, and the hypothesis with the highest likelihood agreement (exploiting the Mahalanobis distance) is assigned to the detection in question. Hypotheses that are the most unlikely tend to be pruned.

The goal of multiple hypothesis testing is to converge on the correct hypothesis by pursuing an abductive/inductive reasoning approach whereby the data are used for their ability to identify and remove the wrong or unlikely hypotheses. This was referred to earlier as the “Moriba Jah Refrigerator Approach.” Any surviving hypotheses at any given time have a statistical likelihood of explaining past observations. The following provide more insight into the difficulties of data association (Fig. 8).

Let us examine the concept of the JPDA. Assume we have two known space objects that we are tracking and we have just received two detections (measurements) as in Fig. 8b. The ellipses surrounding each object represent the object’s uncertainty projected (or transformed) into the reference frame where the measurements are represented, assuming that the uncertainty can be represented as a Gaussian probability distribution. There are many occasions when this is not the case, and thus care must be taken in considering realistic measures of uncertainty. The next, below, shown a comparison of orbital probability mass distribution against uncertainty represented as a Gaussian assumption versus one that allows the representation to adapt to the underlying propagated errors called AEGIS (DeMars et al. 2013). It is seen how the Gaussian error ellipses do not conform to the shape or density distribution of error in the orbital plane. All decisions are based upon the assumed uncertainty, so if it is grossly inaccurate, then only flawed decisions can be the result.

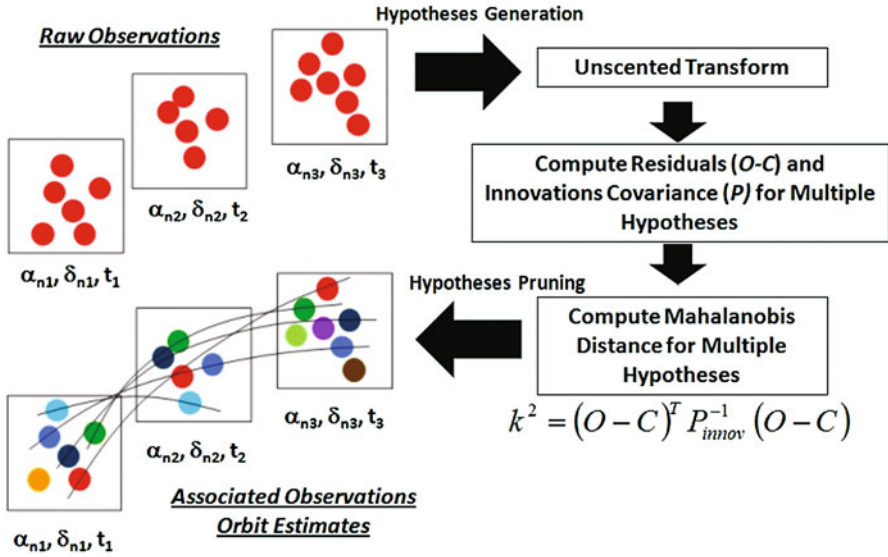


Fig. 7 Data association

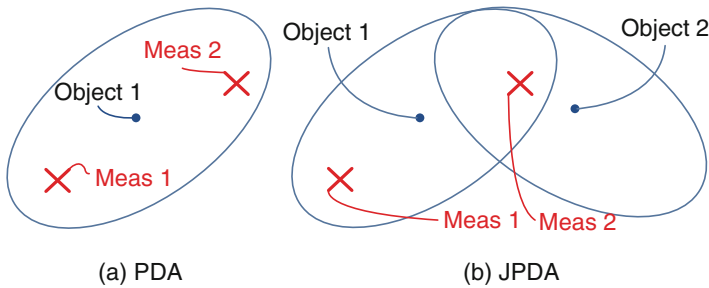
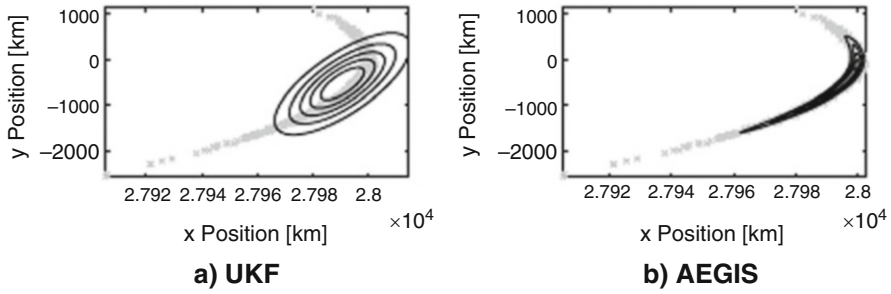


Fig. 8 Probabilistic and joint probabilistic data association

What are the possible joint events or hypotheses that could explain the scenario in the Fig. 9 with multiple hypotheses? Table 1 enumerates these, and all of them could be possible and thus must be considered in the tracking framework. As the number of objects and detections increases, it can be seen that the combinatorics involved invokes the need of computational capacity and efficiency to say the least.

Not considering any of these joint events could lead to errors in the future because we may be missing important information and this could lead to a degraded tracking capability. To this point, there are actually more joint events to consider in the prior scenario that we did not include such as the joint event of measurement 1 having originated from object 2 which performed an unknown (therefore unmodeled) propulsive maneuver. Other domains such as air, ground, etc. may not require an accurate knowledge of the physics because they tend to be data-rich environments



**Fig. 9** Comparison of orbital probability mass distribution against uncertainty representation

**Table 1** JPDA scenario example

Joint event	Marginal events	Object # associated with measurement:		Event Description
		1	2	
$\Theta_1$	$\theta_{0, 1}, \theta_{0, 2}$	0	0	Meas. 1 & 2 from clutter
$\Theta_2$	$\theta_{1, 1}, \theta_{0, 2}$	1	0	Meas. 1 from Obj. 1, Meas. 2 from clutter
$\Theta_3$	$\theta_{0, 1}, \theta_{1, 2}$	0	1	Meas. 1 from clutter, Meas. 2 from Obj. 1
$\Theta_4$	$\theta_{0, 1}, \theta_{2, 2}$	0	2	Meas. 1 from clutter, Meas. 2 from Obj. 2
$\Theta_5$	$\theta_{1, 1}, \theta_{2, 2}$	1	2	Meas. 1 from Obj. 1, Meas. 2 from Obj. 2

(i.e., there are many measurements available). However, the space tracking problem, specifically space surveillance, tends to be data-starved, and thus the physics must be relied upon to properly predict the motion in between sparse observations.

## Summary

In order to develop and maintain a database or catalog of space objects and events, and perform space surveillance and tracking successfully, all of the elements presented in this paper must be brought together very skillfully and effectively. Data must be properly curated, collected, transformed, stored, managed, rectified, fused, exploited, disseminated, etc. Great care must be taken in making assumptions and avoiding the temptation to assume more than what the data and information available allow or indicate. Being successful requires an ability to do the proper “detective” work and learn as much as possible from the data for the purpose of improving one’s predictability of future behavior. Many people can reconstruct events and trajectories, but few can predict them because prediction requires one to know and understand the underlying system. The SDIF model is the framework that drives the entire process, and it should be driven by user needs and requirements. Without the SDIF model, the output of the tracking and surveillance will be less

useful to user needs or may not satisfy them entirely. Of great importance is the ability to quantify and realistically represent the uncertainty of the system. Most people make the assumption that all of the errors are Gaussian, but there is substantive evidence that this assumption is oftentimes flawed, dependent upon the scenario. The focus should be on uncertainty realism versus blindly constraining oneself to Gaussianity. Last but not least, one must understand the data that one is collecting, receiving, and processing. Many errors in what is inferred from the space surveillance activity can be attributed to exploiting measurements under invalid assumptions.

---

## References

- Bever M, Delande E, Jah M (2019) Outer probability measures for first and second order uncertainty in the space domain. IAA-AAS SciTech-040, Moscow, Russia, June
- Delande E, Houssineau J, Jah M (2018) Physics and human-based information fusion for improved resident space object tracking. *Adv Space Res* 62(7):1800–1812. <https://doi.org/10.1016/j.asr.2018.06.033>. Elsevier
- DeMars KJ, Bishop RH, Jah MK (2013) Entropy-based approach for uncertainty propagation of nonlinear dynamical systems. *J Guid Control Dyn* 36(4):1047–1057. <https://doi.org/10.2514/1.58987>
- Stauch J, Bessell T, Rutten M, Baldwin J, Jah M, Hill K (2017) Joint Probabilistic Data Association and smoothing applied to multiple space object tracking. *J Guid Control Dyn* (Special Issue on Space Domain Awareness):1–15. <http://arc.aiaa.org/doi/abs/10.2514/1.G002230>



# Space Security and Frequency Management 51

Yvon Henri and Attila Matas

## Contents

Introduction .....	986
Organizational Structure of the ITU .....	988
Major Principles .....	988
Frequency Allocation Structure .....	989
Regulations Applying to the Use of Frequencies and Orbits by Satellite Networks .....	990
Procedures Applying to Non-planned Space Services .....	991
Advance Publication Information (API) Procedure .....	991
Procedure for Effecting Coordination of Frequency Assignments .....	992
Non-GSO FSS Satellite System: Particular Features .....	993
Notification and Recording in the MIFR .....	995
Bringing into Use of a Satellite Network .....	996
Responsibilities of the Notifying Administration After Recording in the MIFR .....	997
Non-GSO Satellites with Short Duration Mission (SDM) .....	998
BSS Plans and Their Associated Procedures (Appendices 30/30A) .....	999
FSS Plan and Its Associated Procedures (Appendix 30B) .....	999
Administrative Due Diligence .....	1000
Preventing Harmful Interference to Satellite Systems: Non-interference as a Norm .....	1001
Security Aspects and Protection of Frequency Assignments Recorded in the MIFR .....	1002
Conclusion .....	1004
References .....	1004

## Abstract

The International Telecommunication Union (<https://www.itu.int>) (ITU) is unique among UN-specialized agencies in having a mix of public and private

Y. Henri  
OneWeb, London, UK  
e-mail: [yhenri2017@gmail.com](mailto:yhenri2017@gmail.com)

A. Matas (✉)  
Orbit/Spectrum Consulting, Grand-Saconnex, Switzerland  
e-mail: [am@orbitspectrum.ch](mailto:am@orbitspectrum.ch)



sector members. In addition to the 193 Member States, the organization includes also over 800 members comprising the world's leading ICT operators, equipment manufacturers, software developers, service providers, R&D organizations, and local, regional, and international ICT bodies which are approved by the Member State concerned. ITU has three main areas of activity organized in "sectors" which work through conferences and meetings. The Radiocommunication Sector (ITU-R) coordinates this vast and growing range of radiocommunication services, as well as the international management of the radio-frequency spectrum and satellite orbits. The Telecommunication Standardization Sector (ITU-T) is in charge of developing ITU standards (called Recommendations), fundamental to the operation of today's ICT networks. Last but not least, the Telecommunication Development Sector (ITU-D) is in charge of initiatives for ITU's internationally accorded mandate to "bridge the digital divide." For over 150 years, ITU has worked alongside the industry, building global consensus, reconciling competing interests, and forging the new technical standards that have served as the platform for the development of what is now the world's most dynamic business sector.

---

## Introduction

The International Telecommunication Union (<https://www.itu.int>) (ITU) is unique among UN-specialized agencies in having a mix of public and private sector members. In addition to the 193 Member States, the organization includes also over 800 members comprising the world's leading ICT operators, equipment manufacturers, software developers, service providers, R&D organizations, and local, regional, and international ICT bodies which are approved by the Member State concerned. ITU has three main areas of activity organized in "sectors" which work through conferences and meetings. The Radiocommunication Sector (ITU-R) coordinates this vast and growing range of radiocommunication services, as well as the international management of the radio-frequency spectrum and satellite orbits. The Telecommunication Standardization Sector (ITU-T) is in charge of developing ITU standards (called Recommendations), fundamental to the operation of today's ICT networks. Last but not least, the Telecommunication Development Sector (ITU-D) is in charge of initiatives for ITU's internationally accorded mandate to "bridge the digital divide." For over 150 years, ITU has worked alongside the industry, building global consensus, reconciling competing interests, and forging the new technical standards that have served as the platform for the development of what is now the world's most dynamic business sector.

Concerning space services, during the last 56 years, from the first ever World Administrative Radio Conference (WARC-63) (ITU 2019) (<https://www.itu.int/en/history/Pages/RadioConferences.aspx?conf=4.89>) in 1963, up to and including the forthcoming World Radiocommunication Conference, in 2019 (WRC-19)

(ITU 2019) (<https://www.itu.int/en/ITU-R/conferences/wrc/2019/>), many ITU conferences have addressed the regulation of spectrum/orbit usage by stations of the space radiocommunication services. The ITU Member States have established a legal regime which is codified through the ITU Constitution/Convention (ITU 1992) (Constitution of the ITU, 22 DEC 1992, (CS); Convention of the ITU, 22 DEC 1992, (CV)), including the Radio Regulations (ITU 2016) (ITU Radio Regulations, Edition of 2016) (RR). These instruments contain the main principles and lay down the specific regulations governing the following major elements:

- Frequency spectrum allocations to different categories of radiocommunication services
- Rights and obligations of Member administrations in obtaining access to the spectrum/orbit resources; International recognition of these rights by recording frequency assignments and, as appropriate, orbital information for a space station on-board a geostationary satellite or for space station(s) on-board non-geostationary satellite(s), used or intended to be used in the Master International Frequency Register (MIFR) or by their conformity, where appropriate, with a Space Plan

The above regulations are based on the main principles of efficient use of and equitable access to the spectrum/orbit resources laid down in No. **196** of the ITU Constitution (ITU 1992) (Article 44 of the ITU Constitution), which stipulates that *“In using frequency bands for radio services, Members shall bear in mind that radio frequencies and any associated orbits, including the geostationary-satellite orbit, are limited natural resources and that they must be used rationally, efficiently and economically, in conformity with the provisions of the Radio Regulations, so that countries or groups of countries may have equitable access to those orbits and frequencies, taking into account the special needs of the developing countries and the geographical situation of particular countries.”* As indicated in the above provision, further detailed regulations and procedures governing orbit/spectrum use are contained in the Radio Regulations (RR), which is a binding international treaty (ITU 1992) (Article 31 of the ITU Constitution).

Specific procedures have been established to ensure international recognition of the frequencies used and to safeguard the rights of administrations when they comply with those procedures.

The fact that the ITU Constitution and Convention and the RR that complement them are *intergovernmental treaties ratified by governments* means that those governments undertake:

- To apply the provisions in their countries
- To adopt adequate national legislation that includes, as the basic minimum, the essential provisions of this international treaty

---

## Organizational Structure of the ITU

The ITU Plenipotentiary Conference consisting of the representatives of the Member States of the Union is the highest policy-making body of the ITU. Held every 4 years, it is the key event at which ITU Member States decide on the future role of the organization, thereby determining the organization's ability to influence and affect the development of information and communication technologies (ICTs) worldwide. The conference sets the Union's general policies (adoption of the 4-year strategic and financial plans; election of the senior management team of the organization (Secretary General, Deputy Secretary General, and Directors of the 3 Bureaux (Radio-communications, Standardization, and Development)), the Member States of the Council (48 Members states representing the five geographical regions (Americas, Western Europe, Eastern Europe and Northern Asia, Africa, Asia, and Australasia)), and the 12 members of the Radio Regulations Board. The last ITU Plenipotentiary Conference met for the 20th time in Dubai, United Arab Emirates, in November 2018.

The Council, on the other hand, acts as the Union's governing body in the interval between Plenipotentiary Conferences. Its role is to consider broad telecommunication policy issues to ensure that the Union's activities, policies, and strategies fully respond to today's dynamic, rapidly changing telecommunications environment. ITU Council also prepares a report on the policy and strategic planning of the ITU and responsible for ensuring the smooth day-to-day running of the Union, coordinating work programs, approving budgets, and controlling finances and expenditure.

The Radio Regulations Board (RRB) is composed of elected members who are recognized by their qualifications in the field of radiocommunications and their practical experience in the assignment and utilization of radio frequencies. The duties of the RRB are defined in Article 14 of the Constitution and include, inter alia, the approval of the Rules of Procedure (RoP) (ITU 2017) (<https://www.itu.int/en/publications/ITU-R/pages/publications.aspx?parent=R-REG-ROP-2017&media=electronic>) in conformity with the RR and with decisions by radiocommunication conferences, the examination of any other issue that cannot be resolved through the application of the RoP, and any appeals against decisions made by the Radiocommunication Bureau (Bureau) regarding frequency assignments.

---

## Major Principles

In the process of establishing the ITU's space-related regulations, emphasis was laid from the outset on *efficient, rational, and cost-effective utilization*. This concept was implemented through a "first come, first served" procedure. This procedure ("coordination before use") is based on the principle that the right to use orbital and spectrum resources for a satellite network or system is acquired through negotiations with the administrations concerned by actual usage of the same portion of the spectrum and orbital resource. If applied correctly (i.e., to cover genuine requirements), the procedure offers the means of achieving efficient spectrum/orbit management; it serves to

fill the gaps in the orbit(s) as needs arise. On the basis of the RR, and in the frequency bands where this concept is applied, Member administrations designate the volume of orbit/spectrum resources that is required to satisfy their actual requirements. It then falls to the national administrations to assign frequencies and orbital requirements, to apply the appropriate procedures (international coordination and recording) for the space segment and earth stations of their (governmental, scientific, public, and private) networks, and to assume continuing responsibility for the networks.

The progressive exploitation of the orbit/frequency resources and the resulting likelihood of congestion of the geostationary satellite orbit (GSO) prompted ITU Member countries to consider more and more seriously the question of *equitable access* in respect to the orbit/spectrum resources. This resulted in the establishment (and introduction into the ITU regulatory regime) of frequency/orbital position Plans in which a certain amount of frequency spectrum is set aside for future use by all countries, particularly those which are not in a position, at present, to make use of these resources. These Plans, in which each country has a predetermined GSO orbital position associated with the free use, at any time, of a certain amount of frequency spectrum, together with the associated procedures, guarantee for each country equitable access to the spectrum/orbit resources, thereby safeguarding their basic rights. Such Plans govern a considerable part of the frequency bands available for the space communication services.

During the last 56 years, the regulatory framework has been constantly adapted to changing circumstances and has achieved the necessary flexibility in satisfying the two major, and not always compatible, requirements of efficiency and equity. With the dramatic development in telecommunication services, increasing demand for spectrum/orbit usage for practically all space communication services has been observed. This increase is attributable to many factors. These include not only technological progress, but also political, social, and structural changes around the world. Those factors also include their impact on (i) the liberalization of telecommunication services, (ii) the introduction of non-geostationary satellite orbit (non-GSO) satellite systems for commercial communications (large non-GSO constellations as well non-GSO systems with short duration mission), (iii) growing market orientation, (iv) the change in the way this widening market is shared between private, and (v) state-owned service providers and the general globalization and commercialization of communication systems.

---

## Frequency Allocation Structure

The Table of Frequency Allocations (Table) (ITU 2016) (Article 5 of the RR) and associated principles represent a basis for the planning and implementation of radiocommunication services. The current approach is based on a block allocation methodology with footnotes. The regulated frequency band (8.3 kHz–3000 GHz) is segmented into smaller bands and allocated to over 40 defined radiocommunication services (ITU 2016) (Article 1 of the RR). The radio services are identified as *primary* or *secondary* (the latter shall cause no harmful interference to, or claim

protection from, the former) and footnotes are used to further specify how the frequencies are to be assigned or used. The Table is organized into three Regions of the world and is supplemented by assignment and allotment Plans for some bands and services, and/or by mandatory coordination procedures.

Using the Table as a starting point, the frequency spectrum management authority of each country selects appropriate frequencies with a view to assigning them to stations of a given service. Before taking the final decision to assign a frequency to a station in a given radiocommunication service in a given frequency band and to issue an appropriate license, the authority concerned should be aware of all other conditions regulating the use of frequencies in the band concerned, e.g.:

- Are there other mandatory RR provisions governing the use of the frequencies?
- Is the band concerned subject to a pre-established international assignment or allotment Plan? Are the characteristics of the assignment in accordance with the appropriate entry in the Plan? Is there a need to apply the Plan modification procedure prior to issuing a license?
- Is there a need for effecting the coordination procedure prior to notification of the concerned assignment to the Bureau or prior to its bringing into use?
- Is the procedure mandatory or voluntary? Is the procedure specified in the RR or in a special agreement?
- Is there a need to notify the frequency assignment to the Bureau, when should such notification be effected, which characteristics are to be notified, what action should be foreseen after the recording or otherwise of the frequency assignment concerned?

---

## Regulations Applying to the Use of Frequencies and Orbits by Satellite Networks

The specific procedures setting out the rights and obligations of the administrations in the domain of orbit/spectrum management and providing means to achieve interference-free radiocommunications have been laid down by successive WRCs on the basis of the two main principles referred to above: efficient use and equitable access. In order to put these principles into effect, two major mechanisms for the sharing of orbit and spectrum resources have been developed and implemented:

- A priori planning procedures (guaranteeing *equitable access* to orbit/spectrum resources for *future use*), which include:
  - The Allotment Plan for the fixed-satellite service using part of the 4/6 and 10–11/12–13 GHz frequency bands contained in Appendix **30B** (ITU 2016) (Appendix **30B** of the RR)
  - The Plan for the broadcasting-satellite service in the frequency band 11.7–12.7 GHz (Appendix **30**) and the associated Plan for feeder links in the 14 GHz and 17 GHz frequency bands (Appendix **30A**) (ITU 2016) (Appendix **30/30A** of the RR)

- Coordination procedures (with the aim of *efficiency* of orbit/spectrum use and interference-free operation satisfying *actual requirements*), which include:
  - Geostationary satellite networks (in all services and frequency bands) and non-geostationary satellite networks in certain frequency bands governed by the RR No. **9.11A** procedure, which are subject to advance publication and coordination procedures
  - Other non-GSO satellite networks (all pertinent services and certain frequency bands), for which only the advance publication procedure is required before notification

---

## Procedures Applying to Non-planned Space Services

The procedures for non-planned space services are contained primarily in Article 9 of the RR “Procedure for effecting coordination with or obtaining agreement of other administrations.”

The coordination procedure is based on a “first come, first served” principle. Successful coordination of space networks or earth stations gives an international recognition to the use of frequencies by these networks/stations. For such frequency assignments, this right means that other administrations shall take them into account when making their own assignments, in order to avoid harmful interference. In addition, frequency assignments in frequency bands subject to coordination or to a Plan shall have a status conditioned by the application of the procedures relating to the coordination or associated with the Plan. The relevant provisions involve three basic steps:

- Advance publication information (Section I, Article 9) (ITU 2016) (Article 9, Section I of the RR)
- Coordination request (Section II, Article 9) (ITU 2016) (Article 9, Section II of the RR)
- Notification (Article 11) (ITU 2016) (Article 11, Section I of the RR)

---

## Advance Publication Information (API) Procedure

For a satellite network or a satellite system not subject to the coordination procedure, an administration shall send to the Bureau a general description of the network or system for advance publication in the International Frequency Information Circular (BR IFIC) (ITU 2019) (<https://www.itu.int/ITU-R/go/space-brific/en>) not earlier than 7 years and preferably not later than 2 years before the planned date of bringing into use of the network or system (see also No. **11.44** of the RR). The characteristics to be provided for this purpose are listed in Appendix 4 of the RR (ITU 2016) (Appendix 4 of the RR). Upon receipt of the advance publication, administrations should check whether the planned system is likely to affect their existing or planned systems or stations and both administrations shall endeavor to

cooperate in joint efforts to solve any difficulties, with the assistance of the Bureau, if so requested.

The first two steps of the procedure (advance publication and coordination) have been streamlined for GSO networks and non-GSO networks and systems subject to coordination by WRC-15. In the case of GSO networks and non-GSO networks and systems subject to Section II, Article 9 coordination, no requirement to send to the Bureau the advance publication information in addition to the coordination request ones. Upon receipt of the complete coordination information, the Bureau shall publish, using the basic characteristics of the coordination request, a general description of the network or system for advance publication in a Special Section of the BR IFIC.

For some space services commonly used in non-GSO satellite networks not subject to coordination as Earth exploration-satellite service, meteorological satellite service, space research service, space operation service, etc., the administration has to submit advance publication information to the Bureau before the notification procedure, the regulatory final step for the recording of the frequency assignments in the MIFR.

The date of receipt of the advance publication or coordination request information as applicable starts of regulatory 7-year time limit for the frequency assignments of the system to be notified and recorded in the MIFR and brought into use.

---

## **Procedure for Effecting Coordination of Frequency Assignments**

Coordination is a further step in the process leading up to notification of the frequency assignments for recording in the MIFR. The coordination procedure is a formal regulatory obligation both for an administration seeking to assign a frequency assignment to its network and for an administration whose existing or planned services may be affected by that assignment. An agreement arising from this coordination confers certain rights and imposes certain obligations on the administrations concerned; as such, coordination must be effected in accordance with the relevant regulatory procedures laid down in the RR and on the basis of technical criteria either contained in Appendix 5 of the RR (ITU 2016) (Appendix 5 of the RR) or otherwise agreed to by the administrations concerned.

For most coordination cases related to space services, the responsible administration shall send to the Bureau the request for coordination together with the appropriate information listed in Appendix 4 of the RR. On receipt of the request for coordination, the Bureau will promptly examine the information in terms of completeness and conformity with the Convention, the Table of Frequency Allocations and other provisions of the RR (see RoP under No.11.31). The Bureau will then examine the information received in order to identify any administration with which coordination may be needed based on frequency assignments affecting or being affected, as appropriate, and relating to the threshold levels and conditions given in Tables 5-1 and 5-2 in Appendix 5 of the RR.

Finally, the Bureau will publish the complete information (Appendix 4 information and, as appropriate, the names of identified administrations and the specific satellite networks or earth station for coordination between GSO networks with which coordination may need to be effected), in a special section of its BR IFIC.

When a coordination request is received, an administration studies the matter to determine the level of interference likely to be caused to frequency assignments of its networks or stations or caused to assignments of the proposed network or station by its own assignments (No. 9.50 of the RR). Within a total period of 4 months from the date of the publication of the request for coordination in the relevant special section or the date of dispatch of the coordination data, as appropriate, it shall:

- Communicate its agreement to the proposed coordination (Nos. 9.51 and 9.51A of the RR) or
- Provide to the notifying administration (with a copy to the Bureau) the technical data upon which its disagreement is based, along with its suggestions for resolving the problem (No. 9.52 of the RR).

The Bureau's assistance can be requested at the coordination stage of the procedure, by either notifying or objecting administration, with a view to resolving any difficulties which may arise.

As indicated above, there is an obligation for the notifying administration to coordinate with any administration which has initiated the coordination process at an earlier stage. However, there is also a provision (No. 9.53 of the RR) stipulating that both the notifying administration and the objecting administration shall make every possible mutual effort to overcome any difficulties which may arise in a manner acceptable to the parties concerned. The intent of this provision is to facilitate the entry of the newcomer and, even though an administration was first in line, encourage concessions to that end on the basis of mutual cooperation.

---

## **Non-GSO FSS Satellite System: Particular Features**

There is no regulatory definition in the RR related to non-GSO system in the Fixed-Satellite Service (FSS), called time to time also "Mega or Large Constellations," and intended to provide high-speed, low-latency broadband services, including Internet connectivity, throughout the world, including locations which cannot be reached using GSO satellites. A non-GSO FSS system can be considered as "a constellation comprised of a group of satellites, operating in the frequency bands allocated to fixed-satellite service, with similar characteristics and functions, operating in similar or complementary orbital planes under a shared control for coordinated ground coverage."

Typical non-GSO FSS satellite system consists of one or several space stations located on low-Earth orbit (LEO), medium-Earth orbit (MEO), or highly elliptical orbit (HEO) and several gateway stations. The gateways stations purpose is to



connect the non-GSO FSS satellite system with terrestrial networks, to provide each user an access to the private or public networks.

The sharing relationship between GSO networks and non-GSO systems in the FSS and the broadcasting-satellite service (BSS) is covered by the provisions No. **22.2** of the RR (ITU 2016) (Article **22** of the RR), when not otherwise specified in RR:

No. **22.2** § 2 1) Non-geostationary-satellite systems shall not cause unacceptable interference to and, unless otherwise specified in these Regulations, shall not claim protection from geostationary-satellite networks in the fixed-satellite service and the broadcasting-satellite service operating in accordance with these Regulations. No. **5.43A** does not apply in this case. (WRC-07)

In view of the shortage of suitable frequencies, and in order to take advantage of existing space infrastructure and to allow a fair sharing between non-GSO systems and GSO networks in portions of frequency bands allocated to FSS and BSS, WRC-97 and WRC-2000 adopted equivalent power-flux density limits (EPFD) by which an administration operating a non-GSO system in the FSS in compliance with these limits (RR Nos. **22.5C**, **22.5E**, and **22.5F**) shall be considered as fulfilling its obligations under RR No. **22.2** with respect to any GSO networks, provided that operational and additional operational EPFD limits (Tables 22.4A, 22.4A1, 22.4B, and 22.4C) are not exceeded.

There are single-entry limits applicable to non-GSO FSS systems in certain parts of the frequency range 10.7–30 GHz to protect GSO FSS satellite networks operating in the same frequency bands. **RESOLUTION 85** (WRC-03) (ITU 2016) (**RESOLUTION 85** (WRC-03) of the RR) deals with the application of Article **22** to the protection of GSO FSS and BSS satellite networks from non-GSO FSS satellite systems. In accordance with this Resolution and availability of the EPFD validation software, the Bureau is currently able to verify compliance with the limits in Tables 22-1A, 22-1B, 22-1C, 22-1D, 22-1E, 22-2, and 22-3 and to determine the coordination requirements under Nos. **9.7A** and **9.7B** (specific large earth station). Additional protection GSO FSS and BSS from all non-GSO FSS system is described in **RESOLUTION 76** (REV.WRC-15) (ITU 2016) (**RESOLUTION 76** (REV.WRC-15) of the RR) which ensures protection of GSO FSS and BSS networks from the maximum aggregate EPFD produced by multiple non-GSO FSS systems in frequency bands where EPFD limits have been adopted.

This Resolution is instructing that all administrations operating or planning to operate non-GSO FSS systems, individually or in collaboration, shall take all possible steps, including, if necessary, by means of appropriate modifications to their systems, to ensure that the aggregate interference into GSO FSS and BSS networks caused by such systems operating co-frequency in these frequency bands does not cause the aggregate power levels given in Tables 1A to 1D (see RES-76) to be exceeded and in the event that the aggregate interference levels in Tables 1A to 1D (see RES-76) are exceeded, administrations operating non-GSO FSS systems in these frequency bands shall take all necessary measures expeditiously to reduce the aggregate EPFD levels to those given in Tables 1A to 1D (see RES-76).

## Notification and Recording in the MIFR

The procedure for notification and recording of space network frequency assignments in the MIFR is described in Article 11 of the RR. The MIFR represents one of the pillars of the international radio regulatory setup as it contains *all frequency in use or plan to be used notified to ITU*. It should be consulted before selecting a frequency for any new user. For these reasons, *notification of frequency assignments to the Bureau, with a view to their recording in the MIFR, represents the ultimate goal of the frequency registration process and a major obligation for administrations, especially in respect to those frequency assignments that have international implications.*

According to Article 11 provisions, any frequency assignment liable to have an international implication has to be notified to the Bureau:

- If the use of that assignment is capable of causing to or suffering harmful interference from existing or future stations in another country; or if that assignment is to be used for international radiocommunication
- If that assignment is subject to the Article 9 coordination procedure or is involved in such a case
- If it is desired to obtain international recognition for that assignment
- If it is a non-conforming assignment and if the administration wishes to have it recorded for information

For that purpose, administrations submit the relevant characteristics of the frequency assignments to be notified, as specified in Appendix 4 of the RR, to the Bureau. The Bureau shall publish the information in PART I-S of the BR IFIC, thereby ensuring that all administrations are informed of the use of the assignments and that they are taken into account in any future planning conducted at the national, regional, or international level.

The subsequent processing of a notice varies according to the frequency band and service concerned. Each notice is first examined with respect to its conformity with the Table and the other provisions of the RR (regulatory examination); this examination consists in checking that the assignment (frequency, class of station, notified bandwidth) does indeed correspond to an allocation in the Table or the footnotes thereto and, where appropriate, that it complies with other technical or operating conditions laid down in other articles or appendices of the RR (power limits, authorized classes of emission, minimum elevation angle, etc.). If the result of this examination is *unfavorable* and the administration concerned has not explicitly undertaken that the assignment shall be operated subject to not causing interference to assignments operating in conformity with the RR, making reference to No. 4.4 of the RR, the examination stops there and the notice is returned to the notifying administration after publication of the finding in *PART III-S of the BR IFIC*.

When the result of the first examination (under No. 11.31 of the RR) is *favorable*, the assignment is *recorded in the MIFR*, or examined further, if appropriate, from the

viewpoint of its conformity with the coordination procedures (No. **11.32** of the RR) or with a world or regional allotment or assignment Plan (No. **11.34** of the RR).

Following such examinations, the assignment is either recorded in the MIFR and published in *PART II-S of the BR IFIC* (if the finding is *favorable*) or is published in PART III-S of the BR IFIC and returned to the administration (if the finding is unfavorable). The administrations are normally advised to complete the coordination procedure with the identified administrations, or to apply the relevant Plan modification procedure. However, in some specific cases, an administration may resubmit the notice without completing the coordination or Plan modification procedure and the concerned assignment may be recorded in the MIFR under specific conditions.

---

## Bringing into Use of a Satellite Network

One major element of the satellite registration procedure is the respect of the regulatory time limit for bringing a satellite network or system into use (BiU) and submitting notices for recording in the MIFR. No. **11.44** of the RR stipulates that the notified date of bringing into use of any assignment to a space station of a satellite network shall be no later *than 7 years* following the receipt of the advance publication information by the Bureau. WRC-12 defined further bringing into use of a GSO satellite network as contained in RR No. **11.44B** which requires that the “frequency assignment to a space station in the geostationary-satellite orbit shall be considered as having been brought into use when a space station in the geostationary-satellite orbit with the capability of transmitting or receiving that frequency assignment has been deployed and maintained at the notified orbital position for a continuous period of ninety days. The notifying administration shall so inform the Bureau within thirty days from the end of the ninety-day period.” WRC-15 instructed then the Bureau that upon receipt of bringing into use information and whenever it appears from reliable information available that a notified assignment has not been brought into use in accordance with the regulations, the Bureau shall consult the administration for clarification as prescribed in RR No. **13.6**.

Regarding non-GSO systems, no provisions in the RR specifically address the bringing into use issue. It has been the practice of the Bureau to declare their BIU successfully completed when one satellite is deployed into a notified orbital plane and capable of transmitting and/or receiving those frequency assignments. This practice, reflected for FSS and MSS non-GSO systems in section 2 of the RoP for RR No. **11.44**, has been used for a number of years. Furthermore, it has been used irrespective of the number of satellites or of the number of orbital planes indicated in the notification information provided under RR No. **11.2**.

In order to clear the notion of bringing into use for non-GSO systems, the ITU-R has been tasked to study the issue and proposed draft elements in the Conference Preparatory Meeting 2019 (CPM-19) Report for administrations to take a decision at WRC-19, both on the bringing into use of frequency assignments to non-GSO systems and the possibility of adopting a milestone-based approach for the

deployment of non-GSO systems composed of multiple, multi-satellite constellations, in particular frequency bands.

The first general conclusion is that the bringing into use of frequency assignments to non-GSO systems should continue to be achieved by the deployment of one satellite into one of the notified orbital planes within 7 years of the date of receipt of the advance publication of information (API) or request for coordination, as applicable. This conclusion applies for frequency assignments for all non-GSO systems in all frequency bands and services. However, three options are proposed with respect to the minimum period during which a satellite has to be maintained in a notified orbital plane: 90 days (as currently required for fixed-satellite service (FSS) and mobile-satellite service (MSS) non-GSO systems in the RoP for RR No. **11.44**), some period less than 90 days, or no fixed period.

The second general conclusion is that a new WRC Resolution should be adopted to implement a milestone-based approach for the deployment of non-GSO systems in specific frequency bands and services. This milestone-based approach would provide an additional period beyond the 7-year regulatory period for the deployment of the number of satellites, as notified and/or recorded, with the objective to help ensure that the MIFR reasonably reflects the actual deployment of such non-GSO systems. Several options are proposed with respect to the number of milestones, the milestone periods, the required percentage of satellites deployed to satisfy each milestone, the consequences of failing to meet a milestone, and appropriate transitional measures to fairly and equitably address the case of the recorded frequency assignments to non-GSO systems already brought into use, and that have reached the end of their 7-year regulatory period, but where the non-GSO system has not been fully deployed.

The final decision on the bringing into use of non-GSO systems will be taken at WRC-19.

---

## **Responsibilities of the Notifying Administration After Recording in the MIFR**

Recording in the MIFR does not mean the end of activities for the notifying administration as regards the concerned frequency assignment. The notifying administration should remain in close cooperation with the licensing authority and satellite operator and any change in the characteristics of the concerned assignment would have to be notified to the Bureau so as to be reflected in the MIFR, if necessary following additional coordination with the administrations of other countries concerned.

The notifying administration has also to respond to coordination request of any administration which has initiated the coordination process at a later stage with the objective, on the basis of mutual cooperation, to overcome any difficulties which may arise in a manner acceptable to the parties concerned, as stipulated under RR No. **9.53**.

Furthermore, the notifying administration should remain in close contact with the monitoring authority so as to check whether the concerned frequency assignment is operated in compliance with the notified characteristics and whether other elements (e.g., frequency tolerance) are kept within the limits prescribed by the RR. The notifying administration should also initiate appropriate monitoring programs with a view to detecting any operational or technical irregularities in the operation of frequency assignments pertaining to other administrations, and to initiate appropriate actions in this regard, so as to *ensure interference-free operation* for stations under its jurisdiction.

---

### **Non-GSO Satellites with Short Duration Mission (SDM)**

There is currently no regulatory definition for non-GSO SDM satellites. The RR is recognizing only GSO and non-GSO satellites. However, WRC-15 adopted **RESOLUTION 659** (WRC-15) (ITU 2016) (**RESOLUTION 659** (WRC-15) of the RR) Studies to accommodate requirements in the space operation service for non-geostationary satellite with short duration mission, and invited the ITU-R to study the spectrum requirements for telemetry, tracking, and command in the space operation service for the growing number of non-GSO satellites with short duration missions. A new term “short duration mission” (SDM) was used for the first time in the ITU-R, which refers to a non-GSO satellite system having a limited period of validity of not more than typically 3 years. The Resolution invited also WRC-19 to consider the results of ITU-R studies and take necessary action, as appropriate, provided that the results of the studies are complete and agreed by the ITU-R study groups.

Two Agenda Items of WRC-19 were agreed on the non-GSO SDM systems, Agenda Item 1.7 (to study the spectrum needs for telemetry, tracking, and command in the space operation service for non-GSO satellites with short duration missions, to assess the suitability of existing allocations to the space operation service and, if necessary, to consider new allocations, in accordance with **RESOLUTION 659** (WRC-15) and Agenda Item 7 – Issue M – Simplified regulatory regime for non-GSO satellite systems with short duration missions.

In response to the first issue, the CPM-19 Report for administrations to take a decision at WRC-19, developed four methods, and associated regulatory texts to satisfy this agenda item:

- Method A proposes no change to the RR.
- Method B1 proposes a new Space Operation Service (SOS) (Earth-to-space) allocation for non-GSO SD systems in the frequency range 403–404 MHz.
- Method B2 proposes a new SOS (Earth-to-space) allocation for non-GSO SD systems in the frequency range 404–405 MHz.
- Method C proposes to use the SOS allocation in the frequency band 137–138 MHz for downlink and the band 148–149.9 MHz for uplink and to provide appropriate associated regulatory provisions in the RR for telecommand links of non-GSO SD missions.

Regarding WRC-19 Agenda Item 7 Issue M, the studies recognized the specific nature of non-GSO SDM satellite systems being developed by academic institutions, amateur satellite organizations, or by developing countries that are using these satellites to build their expertise in space capability and proposed in the CPM-19 Report for administrations to take a decision at WRC-19 on a draft Resolution – Simplified regulatory regime for non-GSO SDM satellite systems for non-GSO SDM satellite systems, operating under any space radiocommunication service not subject to the application of Section II of Article 9. This draft Resolution recognizes the specific nature of the spectrum allocated to the amateur-satellite service that shall operate in accordance with the definition of the amateur-satellite service as contained in Article 25 (ITU 2016) (Article 25 of the RR) of the RR, resolves the total number of satellites in a non-GSO SDM satellite system constellation shall not exceed [10], and that the maximum period of operation and validity of frequency assignments of a non-GSO SDM satellite system shall not exceed 3 years from the date of bringing into use of the frequency assignments, which is equal to the satellite launch date, without any possibility of extension, after which the recorded assignments shall be cancelled.

---

### **BSS Plans and Their Associated Procedures (Appendices 30/30A)**

Appendices 30 and 30A to the RR contain Plans for the broadcasting-satellite service (BSS) in the 12 GHz band and the associated feeder-link Plans in the fixed-satellite service (FSS) in the 14 and 17 GHz bands. These Plans are occasionally referred to as the “BSS and the associated feeder-link Plans” and were established with a view to facilitating equitable access to the GSO for all countries.

The BSS and associated feeder-link Plans are presented in a tabular form in Articles 10 and 11 of Appendix 30 (hereafter referred to as AP30) and Articles 9 and 9A of Appendix 30A (hereafter referred to as AP30A), respectively. The regulatory procedures associated with the Plans are contained in the Articles of those Appendices. They apply to Plan implementation and modification as well as sharing with respect to terrestrial and other space services in the frequency bands of AP30/30A. Several technical annexes exist containing sharing criteria, calculation methods, and technical data relating to the Plans.

Characteristics of the national assignments, such as nominal orbital position, the service area defined by the ellipse parameters and e.i.r.p. values, and the channel numbers (Frequency assignments) are contained in Articles 10 and 11 of Appendix 30 and Articles 9 and 9A of Appendix 30A.

---

### **FSS Plan and Its Associated Procedures (Appendix 30B)**

Appendix 30B of the RR contains the Plan for the fixed-satellite service (FSS) in the 6/4 GHz frequency bands and in the 13/10–11 GHz frequency bands. This Plan is also referred to as the “FSS Plan” and was established with a view to facilitating equitable access to the GSO for all countries.

The FSS Plan is contained in Appendix **30B** (hereafter referred to as AP30B) together with its associated regulatory procedures. Several annexes exist containing criteria, calculation methods, and technical data relating to the Plan. The FSS Plan is an allotment plan. Each allotment in the Plan comprises:

- A nominal orbital position
- A bandwidth of 800 MHz (uplink and downlink) as listed in paragraph 1 above
- A service area for a national coverage

Characteristics of the national allotments, such as nominal orbital position, ellipse parameters, and power-density values, are contained in Article **10** of AP30B.

---

## Administrative Due Diligence

Following one of the recommendations in the report by the Director of the BR on **RESOLUTION 18** (Kyoto 1994) (ITU 2016) (**RESOLUTION 18** of the RR), WRC-97 adopted **Resolution 49**, which has been modified by subsequent WRCs, on the administrative due diligence applicable to some satellite communication services as a means of addressing the problem of reservation of orbit and spectrum capacity without actual use. This resolution will apply to any satellite network of the fixed-satellite service, mobile-satellite service, or broadcasting-satellite (except in 21.4–22 GHz band) service in frequency bands subject to coordination under Section II of Article **9**, as well as modifications of the Appendices **30** and **30A** Plans and additional uses in the Appendix **30B** planned services.

For the above cases, an administration shall send to the Bureau due diligence information relating to the identity of the satellite network (name of the satellite, notifying administration, reference to the special section publication, frequency range, name of the operator, orbital characteristics) and the spacecraft manufacturer (name of the manufacturer, date of execution of the contract, delivery window, number of satellites procured); this information is to be submitted as early as possible before bringing into use, but must in any case be received before the end of the 7-year period established as a time limit for bringing into use a satellite network. Before notifying its satellite network for recording in the MIFR, the administration shall also send to the Bureau information relating to the launch services provider (name of the launch provider, date of execution of the contract, anticipated launch or in-orbit delivery window, name of the launch vehicle, name and location of the launch facility).

After verifying its completeness, the Bureau will publish the information in a special section of the BR IFIC. Should an administration fail to supply the complete required due diligence information in time, the networks concerned shall be cancelled (cancellation of the coordination request or modification to the Plan or entry in the MIFR) and shall not be recorded in the MIFR.

**RESOLUTION 552** (WRC-12) (ITU 2016) (**RESOLUTION 552** of the RR) contains due diligence procedure for BSS in the band 21.4–22 GHz. The Resolution

is entitled “Long term access to and development in the band 21.4-22 GHz in Region 1 and 3.” The content of this resolution is somewhat similar to **RESOLUTION 49 (ITU 2016)** (**RESOLUTION 49** of the RR) and new data elements are required to be submitted by administration under this Resolution. Under this resolution, administrations have to submit due diligence information not only when the space station is brought into use for the first time but also information about any further change, like deorbiting of the satellite or moving of the satellite to another orbital location. Further, this Resolution requires ITU to provide an ITU-ID for each of physical satellite network brought into use in this band. This satellite ID remains the same for the whole life time of the satellite irrespective of the orbital location of the satellite or its responsible administration until it is deorbited.

---

### **Preventing Harmful Interference to Satellite Systems: Non-interference as a Norm**

In recent years, an increasing number of cases of harmful interference have emerged, including deliberate ones with the intention of disturbing or preventing the reception of signals, which particularly affect telecommunication satellites. In some cases, instances of harmful interference have targeted radio navigation-satellite service (RNSS) signals used by civil aviation, threatening international air traffic with dire consequences including potential loss of life.

A primary objective of ITU is to ensure interference-free operations of radio-communication systems. This has been emphasized at ITU World Radio-communication Conferences, as citizens of every country around the world depend on terrestrial and space radiocommunication systems for the provision of reliable telecommunication and broadcast services. As the leading United Nations agency for management of the radio-frequency spectrum and satellite orbits – and hence responsible for resolving instances of intentional or unintentional harmful interference – ITU is extremely concerned about the growing number of satellite networks which are the targets of deliberate harmful interference. Although currently some mechanisms exist to resolve harmful interference between the parties concerned, a resolution of this nature is often an expensive and lengthy process.

ITU’s response so far has been limited to appealing to all parties that may be involved to exercise the utmost goodwill and to provide mutual assistance in settling issues of harmful interference. In such cases, ITU applies the provisions enshrined in Article 45 (ITU 1992) (Article 45 of the ITU Constitution) of the ITU Constitution and Section VI of Article 15 (ITU 2016) (Article 15 of the RR) of the RR. In most instances, the information provided to ITU by an affected administration includes evidence on the location of the source of harmful interference. However, as the information often comes from a single source, and in the absence of proper means to investigate or corroborate the information, irrefutable evidence cannot be provided to the administration under investigation to assume responsibility for stopping the interference.



Within this context, ITU has signed memoranda of cooperation (MoC) with administrations and organizations that have the capacity to monitor the use of spectrum allocated to satellite services in order to assist us in performing measurements related to cases of harmful interference. A memorandum of cooperation has also been signed between ITU and the International Civil Aviation Organization (ICAO) regarding cases of interference involving the RNSS on board civil aircraft. Such agreements, along with continued work in improving the technical and regulatory environment, are expected to help in the timely settlement of harmful interference cases, including RNSS, which would have a profound impact on improving aviation safety.

To better respond to the satellite interference issue, the Bureau is providing administrations, satellite operators, space agencies, and other space stakeholder member of the ITU-R Sector with an ITU online application “Satellite Interference Reporting and Resolution System” (SIRRS) (ITU 2019) (SIRS: <https://www.itu.int/en/ITU-R/space/SIRRS/Pages/default.aspx>), to be used for reporting and exchange of information concerning cases of harmful interference affecting space services. This online application has been developed in response to **RESOLUTION 186** (Busan 2014) (**RESOLUTION 186** (ITU-PP-14)) and in line with Annex 2 to Decision 5 (Rev. Busan 2014) on modern electronic communication methods. The objective of this system is to facilitate the communication between the parties concerned in case of harmful interference and to assist them in the identification of sources of interference and their prompt elimination in accordance with the provisions of Articles 15 and No. 13.2 of the RR (Articles 13 of the RR) (ITU 2016). The system allows to capture information in accordance with Appendix 10 of the RR and to upload additional information in the format of Report **ITU-R SM.2181** (ITU 2010) (Report **ITU-R SM.2181** <https://www.itu.int/pub/R-REP-SM.2181-2010>), Recommendation **ITU-R RS.2106-0** (ITU 2017) (Recommendation **ITU-R RS.2106-0** <https://www.itu.int/rec/R-REC-RS.2106-0-201707-I/en>) or any other standard format.

---

## Security Aspects and Protection of Frequency Assignments Recorded in the MIFR

According to Article 8 of the RR (Article 8 of the RR), the international rights and obligations of administrations in respect of their own and other administrations’ frequency assignments shall be derived from the recording of those assignments in the MIFR. Any frequency assignment recorded in the MIFR with a favorable finding under No. 11.31 shall have the right to international recognition. For such an assignment, this right means that other administrations shall take it into account when making their own assignments, in order to avoid harmful interference. If harmful interference to the reception of any station whose assignment is in accordance with No. 11.31 is actually caused by the use of a frequency assignment which is not in conformity with No. 11.31, the station using the latter frequency assignment must, upon receipt of advice thereof, immediately eliminate this harmful interference.

In accordance with No. **4.4** of the RR, administrations shall not assign to a station any frequency in derogation of either the Table of Frequency Allocations or other provisions of the RR, except on the express condition that such a station, when using such a frequency assignment, shall not cause harmful interference to, and shall not claim protection from harmful interference caused by, a station operating in accordance with the provisions of the Constitution, the Convention, and the RR. The Regulations recognize therefore the operation of non-conforming stations, however, under strict conditions of non-interference against stations in conformity with the RR, for information purposes only.

Following the RoP on No. **4.4** adopted by the RRB, the scope of No. **4.4** is therefore limited to derogations to the Table of Frequency Allocations. In particular, administrations intending to authorize the use of spectrum under No. **4.4** still have the obligation, under Sections I and II of Article **9**, Nos. **11.2** and **11.3**, to notify to the Bureau “any frequency assignment if its use is capable of causing harmful interference to any service of another administration.” The Board also concluded that administrations, prior to bringing into use any frequency assignment to a transmitting station operating under No. **4.4**, shall determine:

- (a) That the intended use of the frequency assignment to the station under No. **4.4** will not cause harmful interference into the stations of other administrations operating in conformity with the Radio Regulations
- (b) What measures it would need to take in order to comply with the requirement to immediately eliminate harmful interference pursuant to No. **8.5**

When notifying the use of frequency assignments to be operated under No. **4.4**, the notifying Administration shall provide a confirmation that it has determined that these frequency assignments meet the conditions referred to above in item a) and that it has identified measures to avoid harmful interference and to immediately eliminate such in case of a complaint.

The provisions relating either to frequencies or bands to be used for safety and distress communications or allocated for passive usage prohibit any other use:

- (a) Provisions relating to safety and distress communications – in Appendix **15** (Global Maritime Distress and Safety System – GMDSS) (Appendix **15** of the RR), Tables 15-1 and 15-2: frequencies marked with an asterisk (\*) to indicate that any emission causing harmful interference to distress and safety communications is prohibited
- (b) Provisions relating to passive usage – No. **5.340** of the RR (Provision No. **5.340** of the RR)

The Board considers that, in view of this prohibition, a notification concerning any other use than those authorized in the band or on the frequencies concerned cannot be accepted even with a reference to No. **4.4**; furthermore, the administration submitting such a notice is urged to abstain from such usage.

---

## Conclusion

“With a concerted effort, we can reduce, and to the extent possible remove, all obstacles impeding the development and bringing into operation of new satellite networks and systems; we have to think carefully about how we can continue to foster peaceful cooperation among nations through the equitable sharing of global resources and use and improve satellite access to help connect the unconnected, and make the world a better and a fairer place for all” (Henri 2015).

---

## References

- Busan (2014) ITU Plenipotentiary Conference Busan (2014). <https://www.itu.int/en/history/Pages/PlenipotentiaryConferences.aspx?conf=4.294>
- Henri (2015) Orbit/Spectrum international regulatory framework. ITU. [www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2015/October-IISS-2015/Presentations/S1\\_Yvon\\_Henri.pdf](http://www.itu.int/en/ITU-D/Regional-Presence/AsiaPacific/Documents/Events/2015/October-IISS-2015/Presentations/S1_Yvon_Henri.pdf)
- ITU Constitution, 22 DEC 1992, Collection of the Basic Texts of the International Telecommunication Union adopted by the Plenipotentiary Conference. <https://www.itu.int/pub/S-CONF-PLEN-2011>. ITU. Last accessed 09 May 2019
- ITU (2010, 2017) 2017 Rules of Procedure, approved by the Radio Regulations Board. <https://www.itu.int/pub/R-REG-ROP/en>
- ITU Radio Regulations (2016). <http://www.itu.int/pub/R-REG-RR/en>. ITU. Last accessed 09 May 2019
- ITU-R Space Services Department (SSD) <http://www.itu.int/ITU-R/go/space/en>. ITU. Last accessed 09 May 2019
- Kyoto (1994) ITU Plenipotentiary Conference (Kyoto, 1994). <https://www.itu.int/en/history/Pages/PlenipotentiaryConferences.aspx?conf=4.15>



# Space Weather: The Impact on Security and Defense

# 52

Jan Janssens, David Berghmans, Petra Vanlommel, and  
Jesse Andries

## Contents

Introduction .....	1006
Space Weather from the Sun to the User .....	1007
Historical Space Weather Events with Defense and Security Impact .....	1009
Polar Lights as the Ultimate Weapon .....	1010
The Disappearance of the HMS Acheron .....	1010
Jamming Missile Warning Systems .....	1012
Unexpected Detonation of Sea Mines .....	1014
The Battle of Takur Ghar .....	1015
Solar Flares Hampering Hurricane Relief Efforts .....	1017
Space Weather as a Challenge .....	1018
The Research and Observation Challenge .....	1018
The Societal Challenge .....	1019
Specific Defense Challenges .....	1021
Conclusion .....	1023
References .....	1024

## Abstract

Space weather refers to variations induced by the Sun of the Earth's space environment and the impact that these variations can have on technological systems and human health. During space weather events, technology, such as radio communication and GNSS positioning, can be seriously affected. Space weather can cause the loss of satellites, increase radiation levels at aeronautical flight levels and on the ground, and has the potential to catastrophically damage

---

J. Janssens · D. Berghmans (✉) · P. Vanlommel · J. Andries  
Solar Terrestrial Center of Excellence (STCE) – Solar Influences Data Analysis Center (SIDC),  
Royal Observatory of Belgium, Brussels, Belgium  
e-mail: [David.Berghmans@sidc.be](mailto:David.Berghmans@sidc.be)

power grids. We review the space weather cause-effect chains from the source to the affected technologies with special attention to the impact on security and defense.

---

## Introduction

Besides being an exciting scientific discipline, space weather is increasingly recognized as a source of risks to critical infrastructures. Governmental and commercial organizations become progressively aware of their vulnerabilities to the impact of space weather on technological systems and human health. Space weather thereby evolves along the same path as meteorological weather: end users require to be informed on the impact the environment has on their activities, both on average over long time scales as well as operationally in real time.

Most space weather is ultimately due to events in the solar atmosphere such as solar flares, solar energetic particle events, coronal mass ejections, and coronal holes. The impact of these events propagates through interplanetary space and can directly affect technologies and astronauts deployed in space, or indirectly through disturbances of the Earth magnetosphere and ionosphere. Space physics is however only part of the story; the final impact experienced by the end user is critically dependent on the details of the technology and the local environment. Space weather is therefore undeniably multidisciplinary, spanning different space and geophysics as well as engineering domains.

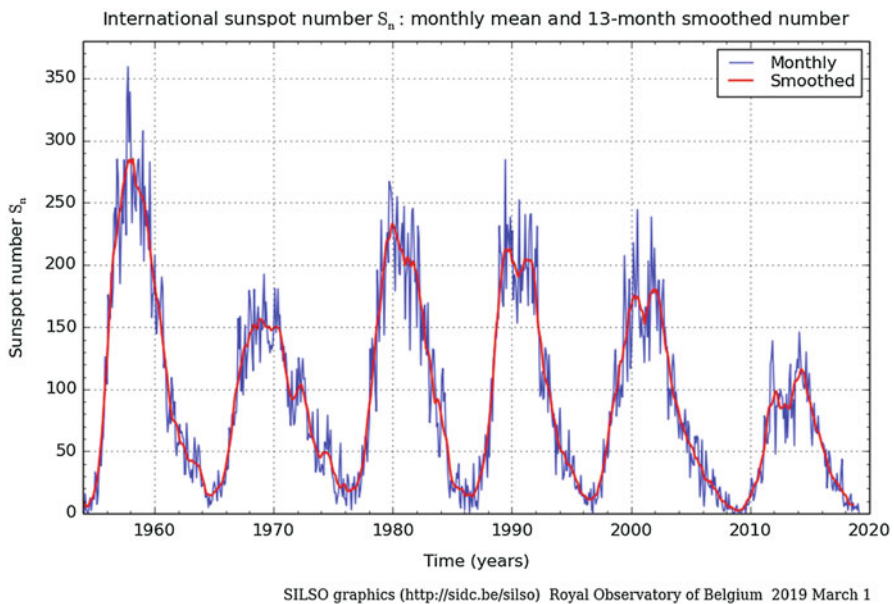
The difficulty with setting up a user-oriented service is that the required space weather and technology expertise is scattered over various disciplines, over many organizations (government organizations, research institutes and companies) in different countries. Several international organizations are therefore taking initiatives to create collaborative frameworks to bring together the required expertise. The World Meteorological Organization (WMO, a specialized agency of the United Nations) has created the Inter-programme Coordination Team on Space Weather (ICTSW) that is tasked to worldwide standardize and enhance the exchange of space weather data and services. In the past years, the Space Situational Awareness (SSA) program of the European Space Agency (ESA) brought together many European space weather assets in a coordinating framework. At the end of 2019, ESA regrouped its space weather activities in a “Space Safety & Security” pillar at the ESA Ministerial Council “Space 19+”.

Section “[Space Weather from the Sun to the User](#)” of this chapter provides an overview of space physics phenomena and the potential impact they have on technologies. This is further illustrated in section “[Historical Space Weather Events with Defense and Security Impact](#)” with a sample of historical space weather events selected for their relevance to security and defense. Section “[Space Weather as a Challenge](#)” addresses the challenges space weather poses for (observational) research, for societal risk handling, and finally as a security and defense issue. The last section provides the conclusions on this chapter on space weather.

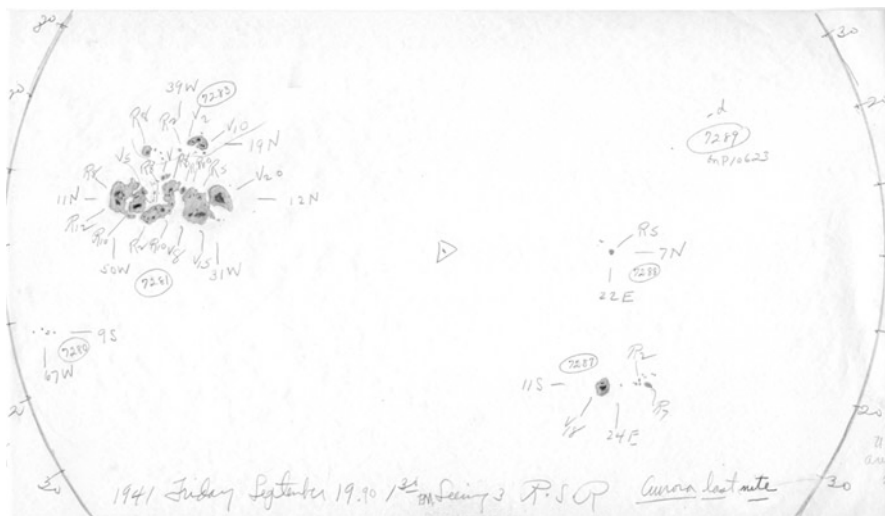
## Space Weather from the Sun to the User

The Sun is a variable star at only 150 million km from the Earth. It is a plasma ball, i. e., a hot ionized gas where the interaction of its electrical and magnetic energy makes its dynamics and variability. Its variability is characterized by the 11-year cycle observed in the counts of the sunspot index (Fig. 1). Sunspots are dark features appearing in groups (Figs. 2 and 4) where the solar magnetic field pierces through the visible surface of the Sun. Higher up in the solar atmosphere, in the solar corona, the sunspots expand in so-called active regions composed of magnetic loops that connect with nearby sunspot groups (Fig. 7). In contrast, in “coronal holes,” the magnetic field is not bundled in strong coronal loops, nor does it reconnect to other place on the solar atmosphere, but expands outwards and fills most of the interplanetary space with the (fast) solar wind. The Sun rotates around its axis in roughly 28 days, with the solar poles taking a few days longer for a complete rotation than the solar equator. Also, the (fast) solar wind is swept around as a fire-hose stream passing by the Earth with 28-day recurrence.

With increasing complexity, the magnetic active regions in the solar corona tend to become unstable to so-called magnetic reconnection thereby producing energy emissions, called solar flares, over the entire electromagnetic spectrum. Solar flares are categorized according to their emission in soft X-rays using a logarithmic scaling (Fig. 8). The most violent class of flares (X-class) amounting to an increase of a factor 10,000 in solar X-ray emission with respect to the background level (A-class)



**Fig. 1** The international sunspot number characterizing the 11-year magnetic activity cycle of the Sun



**Fig. 2** White light drawing from the Mount Wilson Observatory on 19 September 1941, showing the sunspot group responsible for the brilliant aurora the night before. Note the remark from the observer-on-duty in the lower right corner (“Aurora last nite”). The Mt. Wilson 150-Foot Solar Tower is operated by UCLA, with funding from NASA, ONR and NSF, under agreement with the Mt. Wilson Institute (<http://obs.astro.ucla.edu/intro.html>)

observed on quiet days. A similar magnetic reconnection process can lead to coronal mass ejections (CMEs) whereby a large blob of mass is expelled from the solar atmosphere into the solar wind. If the propagation of the CME is faster than the ambient solar wind, then the CME fronts can steepen into shock waves. Solar plasma particles can be accelerated to near-relativistic speeds, either in solar flares or in shock waves. The particles escape away from the Sun into space. Moving through space, these electric particles are forced to follow the magnetic field lines present in the space. These fast particles are called “Solar Energetic Particles” or in short SEPs.

Given its proximity, the Sun drives space weather around the Earth on three timescales:

1. Within 8 min, the electromagnetic radiation emitted by flares and travelling at the speed of light
2. Within an hour, SEPs travelling at near-relativistic speeds from flares or CME shocks
3. Within a day, the bulk mass of the fastest CMEs (~2000 km/s)

Life on the Earth’s surface developed experiencing little or no influence from the above-mentioned solar drivers of space weather because the Earth is surrounded by different protecting layers. The magnetic field of the Earth expands outwards in space and creates a magnetic bubble (the magnetosphere) from which the solar wind

is deflected. Under the pressure of the solar wind, the magnetosphere is deformed on the sun-light “day” side but remains big enough in normal conditions to expand beyond the orbit of geostationary satellites. Under the impact of CMEs or fast solar wind stream however, the magnetosphere temporary further deforms and later resettles. This process is called a geomagnetic storm and is often associated with aurora near the magnetic poles. In the northern hemisphere, these polar lights are most often seen from Scandinavia, Canada, Alaska, and Siberia. By creating large-scale induction currents, geomagnetic storms can also lead to power grid collapse. On longer timescales, geomagnetic induction currents through oil pipelines lead to enhanced corrosion.

The top layer of the Earth atmosphere (roughly from 60 to 1000 km) protects us from extreme ultraviolet (EUV) and X-radiation from the Sun and is called the ionosphere. The ionosphere reflects HF (high frequency) radio waves and is therefore important for radio communication. The ionosphere is a reactive environment which can be strongly influenced by solar flares, by geomagnetic storms and by solar energetic particles. Disturbed ionospheric conditions can lead to HF radio blackouts, degraded satellite communication, and GNSS (Global Navigation Satellite Systems) positioning errors. Under the influence of solar radiation, satellites in low Earth orbit can experience enhanced drag at times the ionosphere is “thickened.”

Solar energetic particles reach the Earth environment at near-relativistic speeds along the interplanetary magnetic field embedded in the solar wind. They are an immediate risk to astronauts and spacecraft electronics. They are deflected by the Earth magnetosphere towards the magnetic poles of the Earth where they collide with atmospheric particles creating a shower of secondary radiation. The most energetic SEP events can however strike anywhere on the Earth with their shower of secondary radiation reaching the ground (so-called ground-level events, GLEs). During such strong SEPs, airplane crew and passengers risk ionizing radiation, and notably during polar flights.

Not unlike earthquakes, space weather events are exponentially distributed with small events being much more numerous than large events. The largest events in recorded history are referred to as extreme space weather. Among geomagnetic storms, the classical reference is the “Carrington event” in 1859 which made telegraph systems, the most advanced technology at the time, fail all over Europe and North America. If such an event would happen again, modern technology would be catastrophically affected. The chance for such extreme events to occur again in the next 10 years is only 12% (Riley 2012). Cases of extreme space weather are thus high impact-low probability events.

---

## **Historical Space Weather Events with Defense and Security Impact**

In this section, we first give an historical account of some noteworthy space weather events with military impact.



## Polar Lights as the Ultimate Weapon

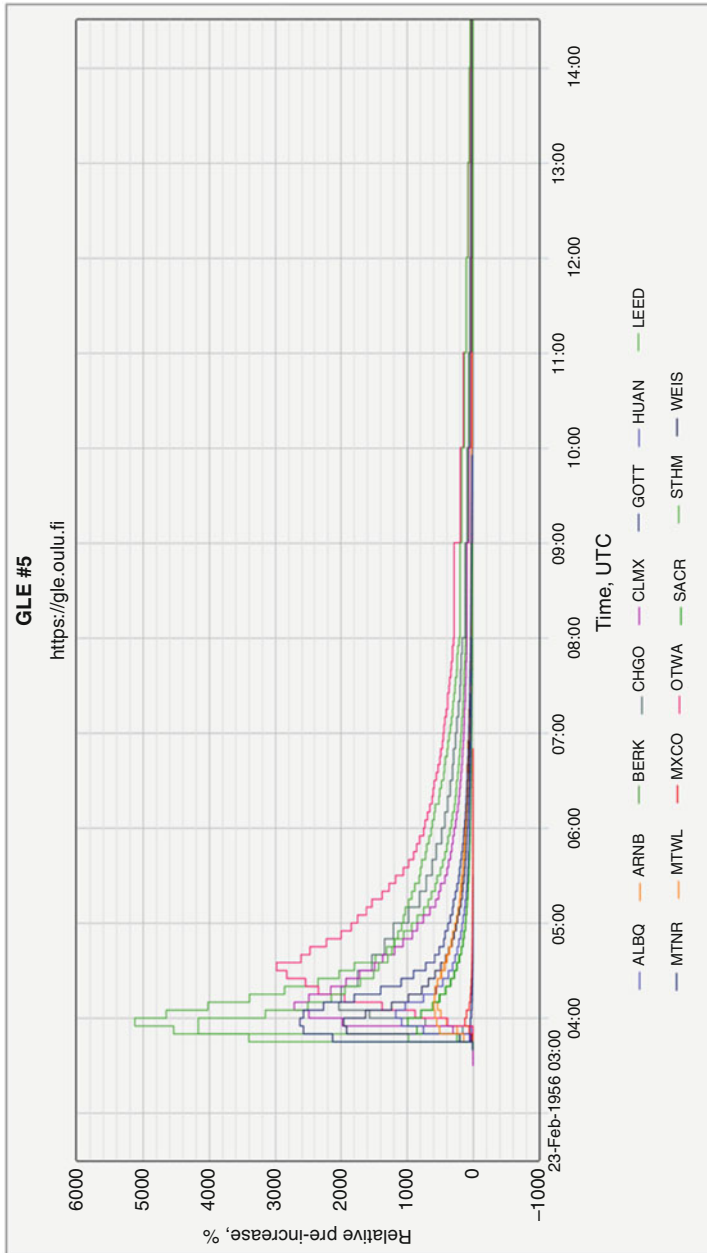
During the Second World War, both belligerent parties made use of the bright shine of the polar lights to attack critical assets of the adversary. A noteworthy example took place in September 1941 (Love and Coïsson 2016). Greenwich sunspot group 1,393,703 appeared from behind the eastern solar limb on 10 September. During its 2-weeks transit over the solar disk, it continued to grow in size and complexity, making it all the way into the Top 50 of largest sunspot groups of the last 170 years! The region was very flare active, and a particularly strong eruption over this sunspot group was observed with the Greenwich Observatory spectroheliograph in the morning of 17 September. Barely 20 h later, magnetometers on Earth went haywire when what is now known as a coronal mass ejection (CME) struck the earth's magnetic field. Starting around 09:00 UT on 18 September, severe to extremely severe geomagnetic storming levels were continuously recorded for a period of 24 h, a level of geomagnetic activity that has not since been matched (Cliver and Svalgaard 2004). The resulting aurora was observed as far south as New Mexico and California (Fig. 2). In Chicago, motorists parked on the highways had caused a traffic jam as they sought a clear view of the celestial spectacle. The press used literary one-liners such as “celestial pyrotechnics,” “neon lights,” or “ethereal blitz” to describe the impressive event. Some citizens even wondered if a new type of anti-aircraft search battery was being tested.

The true effects on war took place in Europe, where the British Royal Air Force carried out a raid on a German supply base in the Baltic Sea, whereas the Germans bombarded Leningrad, each under the lights of the aurora borealis. In the North Atlantic, German U-boats were operating to sink eastbound ships supplying Great Britain. During the night of 18–19 September, the captain of the U-74 recorded in his war diary that the conditions were “as bright as day.” An allied convoy consisting of cargo ships and accompanying anti-submarine warships (“corvettes”), which normally would have been hidden in the dark of night, was detected. Just a few hours later, a decisive torpedo was fired hitting the corvette HMCS *Lévis*, nearly cutting the vessel in two. Shortly afterwards, the HMCS *Lévis* sank leaving many casualties.

## The Disappearance of the HMS *Acheron*

Since the start of the measurements in the early 1940s, only 72 GLEs have been recorded, qualifying them as rare. The strongest GLE occurred on 23 February 1956, and increased radiation levels on several locations by several thousands of percent (Bieber et al. 2005; Fig. 3).

Coincidentally, the HMS *Acheron*, a submarine of the Royal Navy, was performing arctic trials in the Denmark Strait between Iceland and Greenland. The 1,123-ton *Acheron* was a sister ship of the *Affray*, which sank in the English Channel a few years earlier, leaving many casualties. When the *Acheron* did not respond to a routine radio check on 24 February at 10:05 a.m., the Admiralty flashed a “sub-sunk” order, signaling an immediate search with all available ships and planes. Royal



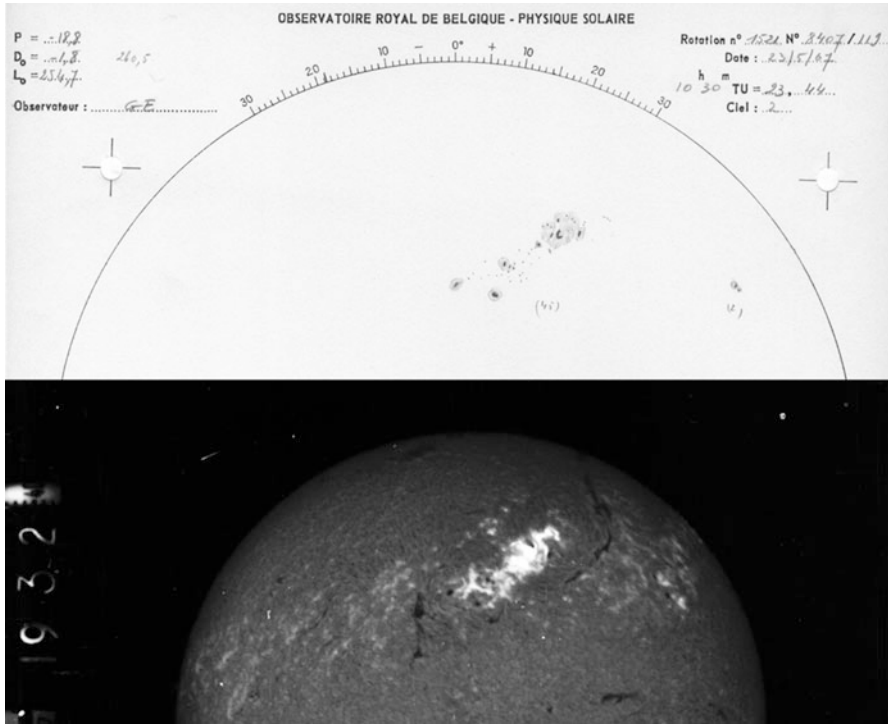
**Fig. 3** On 23 February 1956, neutron monitors around the world recorded a strong increase in neutron counts, what turned out to be the strongest ground-level enhancement ever recorded. A GLE is a rare event with only 72 registrations since the start of the observations in the early 1940s. Most GLEs do not reach 100% in neutron counts increase, corresponding here to halfway between 0% and the first gridline (200%). This testifies of the formidable strength of the 1956 event. Plot from the Oulu Cosmic Ray Station of the University of Oulu, Finland (<https://gle.oulu.fi/#/>)

Air Force planes roared off for Reykjavik, Iceland, to set up a base for search operations. U.S. Air Force units on Iceland already were standing by. Ships steamed out from Scotland and Iceland. Three hours later, the British minesweeper *Coquette* radioed that she had made “visual contact” with the sub in gale-swept seas. The *Acheron* then proceeded to Iceland, and the Admiralty called off the search for the British submarine, which was feared lost for nearly 6 h. It was quickly pointed out that the unusual sunspot activity over the past 2 days might have been the cause of the radio blackout, as gigantic explosions on the Sun had bombarded the Earth with cosmic rays, interfering with communications. In Copenhagen, the Danish government’s telegraph authority said no radio messages had been received from Greenland stations since early morning on 23 February. “Frankly,” a spokesman for the authority said, “we cannot see how a vessel could get signals through while we cannot receive a word from powerful land stations.” (from the “*Amsterdam Evening Recorder*,” 24 February 1956).

### Jamming Missile Warning Systems

In 1967, the Cold War between the Soviet Union with its satellite states (USSR) on the one hand and the United States and its allies on the other hand was in full swing. The USA had a stockpile of more than 30,000 nuclear warheads, while the USSR was making a recovery effort to exceed that number. Ballistic missiles that could carry such warheads were deployed at an increasing pace, and radar systems to detect such missiles were being operated. Tension was high and pushed even further by the ongoing race to the Moon, the continued launch of spy satellites, and other conflicts such as between Egypt and Israel. It was against this backdrop of geopolitical and military turmoil that a large and complex sunspot group appeared at the Sun’s east limb on 17 May. Further increasing in size during the next days, the region started strong flaring activity from 21 May onwards, which would last for a full week. The strongest flare (X6) took place on 23 May around 18:46 UT, which was at sunset for European countries, but near local noon for the central United States (Fig. 4). It was followed by another strong flare (X2) at 19:53 UT. These extraordinary solar eruptions manifested themselves very strongly over all portions of the electromagnetic spectrum, and extreme, hours-long solar radio bursts (i.e., burst in the radio part of the solar spectrum) were recorded. At frequencies of 606 MHz, peak flux densities reached 373,000 sfu (solar flux units), making it the strongest solar radio burst observed up to that time, and of the entire twentieth century. For comparison, typical values for the “undisturbed” flux density at this frequency are somewhere between 30 and 45 sfu.

The solar radio bursts significantly disturbed the United States’ Ballistic Missile Early Warning System, BMEWS for short (Knipp et al. 2016). This radar system operated at 440 MHz from sites in Alaska, Greenland, and the United Kingdom. During the 23 May event, all the BMEWS radar systems had a good view on the Sun, with the Greenland radar particularly well aligned. In response to the solar radio bursts, the radar screens showed many “impacts” which were subsequently interpreted as



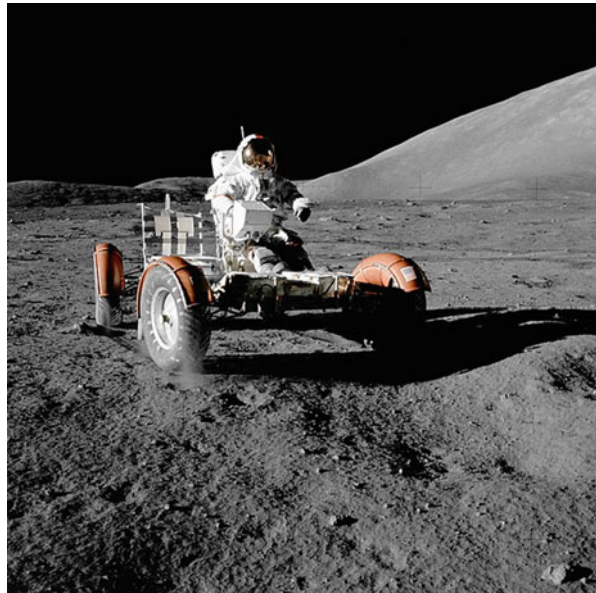
**Fig. 4** The famous sunspot group responsible for the very high solar activity on May 1967. On top, a white light drawing by the USET solar telescope (Royal Observatory of Belgium, Brussels, <http://www.sidc.be/uset/>) on 23 May (10:30 UT). The bottom picture is an H-alpha image taken on 19:32 UT at Sacramento Peak when the X6 flare was still in progress. The size of the bright flare ribbons, covering most of the sunspot group, testifies of the strength of the event (Image from the Flare Patrol H-alpha instrument, NSO/AURA/NSF, [ftp://nispdata.nso.edu/flare\\_patrol\\_h\\_alpha\\_sp/movie/56/](ftp://nispdata.nso.edu/flare_patrol_h_alpha_sp/movie/56/))

jamming by the operators who had never witnessed such an intense radio event. Logically, Cold War military commanders viewed full-scale jamming of surveillance sensors as a potential act of war and positioned their bombers in a ready-to-take-off position. The decision to launch or not to launch is well worth noting, because in view of the tense political situation in May 1967, a full-scale aircraft launch by the allied forces could have been very provocative and, just as importantly, difficult (if not impossible) to abort in view of the impaired radio communications. Fortunately, and despite the limited data available at the time, solar forecasters from the USAF Air Weather Service were able to extract sufficient information from solar and radio observations to convince high-level decision makers at NORAD (North American Air Defense) that the Sun was the likely culprit in contaminating the BMEWS radar signals. This key element defused the critical situation, and the decision was taken to return aircraft and alert status to their normal levels. Further details on this event and its space weather impacts, as well as on the effects from the related extremely severe geomagnetic storm, can be found in Knipp et al. (2016).

## Unexpected Detonation of Sea Mines

Over the years, the solar storm of 4 August 1972 has reached a legendary status among space weather scientists. This storm was very similar to the famous Carrington event in 1859, except for the aurora which was not seen from low geomagnetic latitudes. The main eruption took place during the morning of 4 August and was accompanied by a powerful proton event that reduced the life expectancy of solar panels aboard satellites with no less than 5 years. Yet, things could have been much worse. Indeed, the storm occurred right between the Apollo 16 and 17 missions. If astronauts had been walking on the Moon when this proton event took place, then they would most likely have suffered radiation sickness (Cucinotta et al. 2010; Fig. 5). The CME accompanying the eruption still holds the record for being the fastest CME travelling the Sun-Earth distance. No CME has ever done better than 14.6 h (Cliver and Svalgaard 2004). This achievement was most likely the consequence of eruptive activity during the hours and days prior to the main eruption, clearing the path for the powerful 4 August CME. When it arrived at Earth, the magnetopause, usually at about 10 Earth radii distance, was pushed back to the Earth to only about 5 Earth radii, suddenly exposing several satellites to the wrath of the disturbed solar wind. As the subsequent geomagnetic storm unleashed all its power, some of the magnetometers on Earth went off-scale, and aurora was bright enough to cast shadows. As just recently revealed by the scientists (Knipp et al. 2018), this severe geomagnetic storm had also another effect which had been buried in the military archives for more than 40 years. Indeed, back in 1972, the United States were at war with Vietnam. In an attempt to isolate North Vietnam from

**Fig. 5** Astronaut Eugene A. Cernan checking out the Lunar Roving Vehicle (LRV) during the Apollo 17 mission in December 1972 (Credits: NASA). Just a few months earlier, energetic particles released during a strong solar eruption would have caused radiation sickness if any astronauts had been walking around on the lunar surface at that time



the rest of the world, magnetic-influence sea mines (“Destructors”) had been dropped into the coastal waters of North Vietnam just 3 months prior. On 4 August, aircrews reported the sudden detonation of some two dozen of sea mines near Hon La in just 30 s. Aerial observations indicated evidence of some 4000 additional detonations along the North Vietnamese coast during the first weeks of August. The US Navy quickly concluded that the magnetic field variations were the cause of these detonations, in line with measurements from magnetometers in nearby locations such as Manila, the Philippines. This conclusion led to the radical decision to replace all the magnetic-influence-only sea mines with magneto/seismic mines, meaning there were now two triggers needed before the sea mines could detonate.

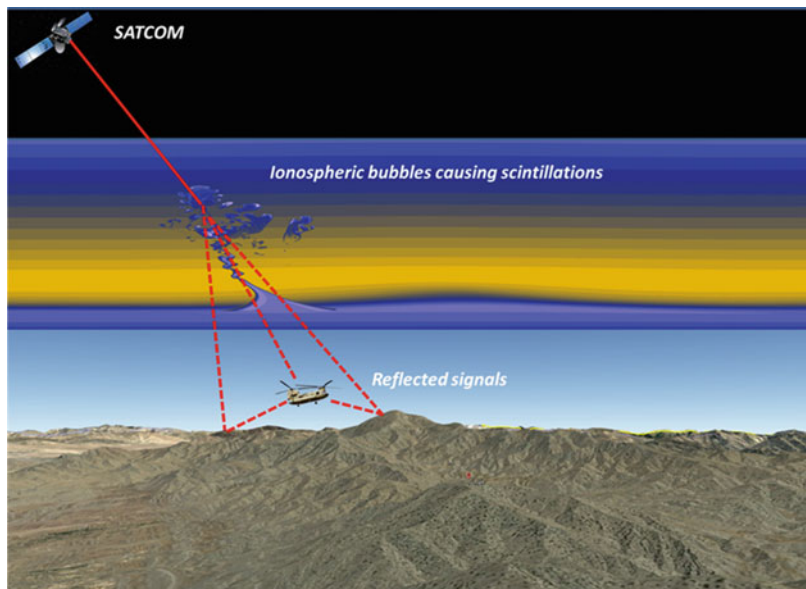
## The Battle of Takur Ghar

So far, the cited examples took place during record setting space weather storms. However, the following case illustrates that even mild disturbances, enhanced by a series of unfavorable conditions, can also lead to insecure situations.

Operation Anaconda took place in Afghanistan from 1 to 18 March 2002. It was a large-scale international military campaign led by the United States aiming at the destruction of Al Qaeda and Taliban forces. An intense battle took place during the morning hours (before dawn) of 4 March on Takur Ghar, a 3191-m high mountain top, as US Special Operations Forces came under heavy fire from the Al Qaeda and Taliban forces. A Chinook helicopter was directed to rescue the team. However, in view of the rocket-propelled grenades and heavy machine guns that the insurgents were using, a SATCOM (Satellite Communications) message was sent to the Chinook to avoid the mountain top. Unfortunately, and despite repeated attempts, the Chinook helicopter never received that critical message. It landed on the top of Takur Ghar and came immediately under intense fire, resulting in several casualties.

A subsequent analysis of the incident blamed the radio outage on poor performance of the UHF (ultra high frequency) radios on the helicopters as well as on terrain radio interference. However, in 2014, Michael Kelly and his team of researchers from the John Hopkins University came to a different conclusion, offering a viable alternative for the outages (Kelly et al. 2014). Utilizing a model that uses UV (ultraviolet) data from the TIMED spacecraft to retrieve the 3D electron density, they came to the conclusion that a combination of ionospheric disturbances with multipath effects (multiple radio reflections from the mountainous terrain) could also have caused the decreased communication links (Fig. 6).

The main cause of the ionospheric unrest is the presence of equatorial plasma bubbles, i.e., depletions of electron density in the ionosphere. Their number correlates with the solar activity level, and they also are more numerous during the equinoxes (spring and autumn) than during the solstices (summer and winter). They usually form after sunset at the bottom of the F-region (main ionospheric layer), where small low-density irregularities can grow into turbulent bubbles. The bubbles have a typical size of about 100 km and their effects usually end around midnight. They can occur during relatively minor levels of geomagnetic activity,



**Fig. 6** Sketch prepared by ROB/GNSS (Dr. Nicolas Bergeot) with Dr. Yokoyama’s model (NICT/AERI) as base. It shows how a combination of ionospheric disturbances (“scintillation”) with reflected signals from the surroundings can weaken and effectively blacken out radio signals from space- or ground-based transmitters

especially during solar cycle maximum. Radio wave propagation can be severely affected in terms of power and intensity as these waves travel through small-scale structures in the ionosphere (i.e., scintillation of radio waves).

At first sight, one would expect relatively strong geomagnetic activity to explain the ionospheric disturbances, but this was not the case on 3–4 March. Quiet to unsettled geomagnetic conditions were observed, with a single active episode during the 21:00–24:00 UT interval on 3 March. According to Kelly and his team, this suppressed the generation of the evening-side depletions and delayed the onset of the ionospheric bubbles until after midnight.

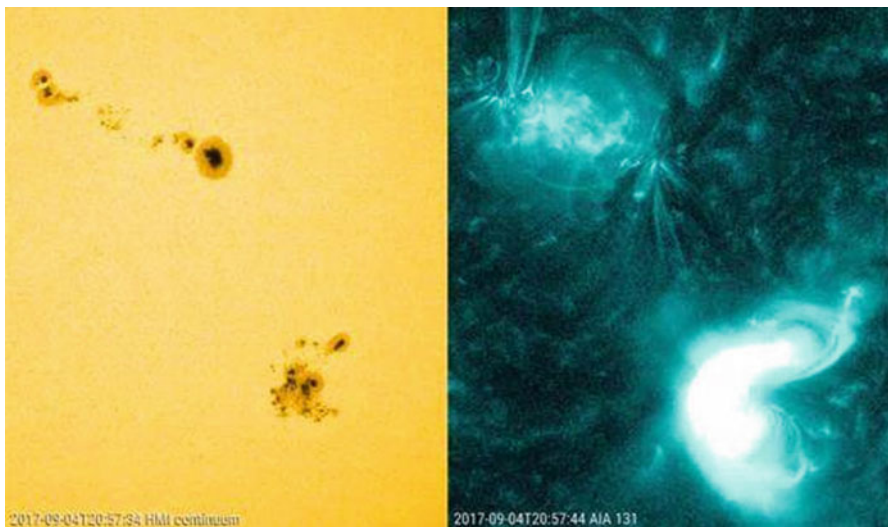
Moreover, analysis of the data from the TIMED satellite led Kelly and his team to conclude that the plasma bubbles affecting the Takur Ghar war theater did not have very steep density gradients, and thus would have resulted only in mild ionospheric disturbances. Normally, this mild ionospheric “scintillation” is not a problem for SATCOM, but the intensity of the already weakened radio signals could have further been reduced by the multiple reflections from the surrounding mountains. Hence they concluded that “. . . the destructive multipath interference from complex terrain reflections coupled with scintillation could cause a signal blackout. . .”. The take-home message here is that even mild disturbances, under a set of unfavorable conditions, can create dangerous situations and that users should always be very attentive.

## Solar Flares Hampering Hurricane Relief Efforts

To conclude the summary of historical space weather impacts on the military operations and technology, we discuss this last recent case to illustrate that sometimes, it's just a matter of unfortunate timing.

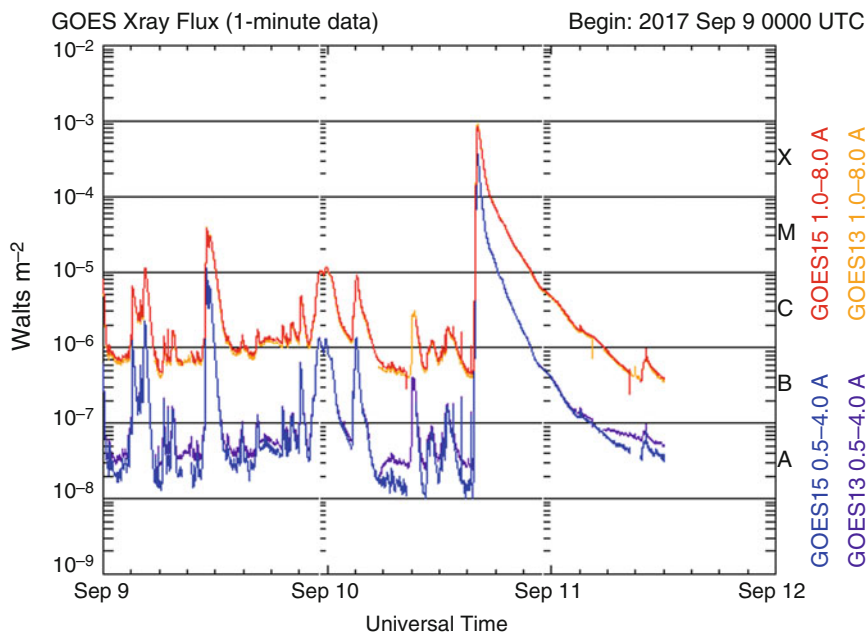
The 2017 Atlantic hurricane season was one of the deadliest and most catastrophic hurricane seasons in recent history, with a damage total exceeding \$200 billion (USD). One of the strongest hurricanes was hurricane Irma, ravaging the Caribbean island chain from the northern Leeward Islands, via Puerto Rico and Cuba to Florida from 6 till 11 September. Coincidentally, from 4 till 11 September, Active Region 2673 (Fig. 7) developed on the solar disk into a complex and very active sunspot group, producing no less than 27 medium and 4 extreme solar flares, including the two strongest flares of the entire solar cycle 24, resp. an X9 on 6 September and an X8 on 10 September (Fig. 8). The numbers of the active regions are determined by the National Oceanic and Atmospheric Administration, NOAA.

These strong flares induced a rapid ionization of the equatorial upper atmosphere, resulting in a disruption of HF communications while emergency workers were struggling to provide critical recovery services to the Caribbean communities (Redmon et al. 2018). The Hurricane Weather Net (HWN) reported that the 6 September solar flare caused a near-total communications blackout for most of the morning and early afternoon. The French Civil Aviation authorities also reported that HF radio contact was lost with an aircraft off the coasts of Brazil and French Guyana



**Fig. 7** A picture of Active Regions NOAA 2674 and NOAA 2673 (right) on 4 September 2017, as imaged by the Solar Dynamics Observatory (SDO) in white light (left) and in extreme ultraviolet (right). A medium-class flare was in progress in NOAA 2673 at that time. Image courtesy NASA/SDO, AIA and HMI science teams. SDO is the first mission for NASA's Living With a Star (LWS) Program





**Fig. 8** The X8 solar flare of 10 September 2017 as measured in soft X-rays by the GOES13 and GOES15 satellites. Flares are categorized as A, B, C, M, or X-class flares. Each class ranges from 1 to 9. Image courtesy NOAA/GOES

for approximately 90 min, triggering an alert phase until a position report was received by New York radio. The 10 September flare also severely disrupted HF communication, with a widespread communication blackout lasting for nearly 3 h, which basically could not have happened at a worse time. The researchers conclude that “. . . These solar eruptions led to geoeffective space weather impacting radio communications tools used in the management of air traffic as well as emergency-and-disaster assessment and relief, temporarily complicating an already extreme terrestrial weather period.” (Redmon et al. 2018). Further reading on Hurricane Irma is found in ► [Chap. 39, “Satellite EO for Disasters, Risk, and Security: An Evolving Landscape”](#).

## Space Weather as a Challenge

### The Research and Observation Challenge

The above two sections illustrate how the cause-effect chains are coupled over different physical domains from the Sun to the Earth. Many links in these cause-effect chains are poorly understood and space weather, or solar-terrestrial physics,

remains thus an active field of research. As compared to meteorological weather, progress in space weather is hampered by the difficulty of obtaining constraining measurements. Measurements of space weather conditions start from observing the Sun, which are necessarily performed from a distance. These “remote sensing observations” (images or timelines) can only be obtained from ground-based telescopes during daytime in wavelengths not hindered by the Earth’s atmosphere (radio and visible parts of the spectrum). Studies of the sources in the solar corona require observations in X-rays or EUV, which can only be observed by satellites outside the Earth’s atmosphere. Even then, only one perspective on the solar globe is obtained and a full 360° view requires several more satellites in deep space observing the Sun from other viewpoints.

The propagation of solar wind plasmas and energetic particles throughout the interplanetary space on their way to the Earth can be confirmed by in situ measurements, but the only stable place between the Sun and the Earth is the Lagrange L1 point where the Sun’s and Earth’s gravitation balance. Unfortunately, following the relative difference in masses, this L1 point is at only 1% of the Earth-Sun distance from the Earth, providing very little warning time for upcoming solar wind disturbances. Further near-Earth in situ space measurements are required to track the state of the magnetosphere and to measure energetic particle fluxes at the top of the atmosphere. The Earth ionosphere is traditionally observed with ionosondes from the ground or through analysis of signals from GPS satellites. Finally, additional observations from the ground are required to measure deflections of the Earth magnetic field during geomagnetic observations. GLEs are confirmed with neutron monitor measurements.

The above list of measurements is only the tip of the iceberg and many additional measurements are possible and probably required to improve scientific understanding. A COSPAR working group has produced a road map for space weather. This report also highlights the importance of another set of measurement data, those of the impacts within the technologies. Measurements of radiation doses at flight altitudes during solar storms or induced currents in the power grid are much less readily available than the corresponding geospatial space weather measurements. Also, in the realm of observed impacts on satellite operations, data are generally not released publicly.

## **The Societal Challenge**

Space weather poses risks to global society, with some regions (e.g., high latitude zones) and some sectors (e.g., those dependent on high precision GNSS) more affected than the others. A proper response to the involved risks will thus differ from region to region and from sector to sector but will require in any case the following elements:

- Understanding of the vulnerabilities, including impact and likelihood
- Preparedness through improved engineering of the affected systems

- Maintaining awareness of the current state of the space environment through observations and analysis in real time

### **Understanding of the Vulnerabilities**

The first step towards a proper handling of the space weather risk within a sector is to have a proper understanding of the (potential) impacts and their likelihood. It is important to note that the exact impact of the space weather phenomena on technological systems goes well beyond space physics and is to a large extent an active separate area of (technological) research. While the physical principles are understood and often historical examples are known to exist (see above), it is much harder to accurately estimate the exact magnitude of the impacts and, more importantly, the associated cost and consequences.

Also, in the case of extreme space weather, one faces the problem of high impact-low probability events which are so rare that proper statistics on impact, cost, and consequences cannot be accumulated (Eastwood et al. 2017). Nevertheless, over the last decades, the understanding of the vulnerabilities has grown substantially in many sectors. Several countries around the world have also explicitly included space weather within their national risk assessments and have accounted for space weather phenomena within their national and sectoral risk management strategies.

### **Preparedness Through Improved Engineering**

When potential impacts are known, there are broadly two venues in order to mitigate the impacts. The first is an engineering solution where the design of the technology is altered such as to become immune or at least less prone to impacts caused by space weather. For example, with sufficient “shielding,” damage to spacecraft electronics by Solar Energetic Particles can be strongly reduced. GNSS positioning errors due to ionospheric variability can to some degree be addressed with dual frequencies or augmentation systems. Such engineering solutions are typically relatively successful for most mundane space weather events but become prohibitively expensive (or even physically impossible) for the most seldom but extreme space weather events.

### **Maintaining Awareness**

When improved engineering or system hardening is not possible, the second strategy is to learn to live with the impacts but reduce their consequences through maintaining active awareness of the current and anticipated space weather conditions, and by actively feeding such information into the operation procedures within each affected sector. As just one example, the International Civil Aviation Organization (ICAO, a specialized agency of the United Nations) has recently identified world space weather information providers that will issue from autumn 2019 onwards so-called advisories to inform aviation actors on the ongoing space weather impacts on HF communication, GNSS positioning, and radiation levels at flight altitudes.

If this second mitigation strategy is followed, one must be aware that the observational challenge highlighted above becomes yet more stringent as the data must be acquired and processed in real time, which is not the case when the

observation data are used for research and model development. Given the implied costs, there is a strong case to be made for international cooperation, both for ground-based observations and for observations from satellites. In the case of ground-based observations, there are additional logistical reasons to make observations from multiple sites across the global. Ground-based solar observations require observatories in different time zones and ionosphere and surface geomagnetic field data require spatial resolution.

### **International Coordination of Space Weather Services**

But maintaining awareness of space weather conditions requires more than just having the observational data available. In addition, models to forecast (near) future behavior and human-based assessment of the meaning of the incoming are needed. It also includes deriving more tailored and focused services for specific users based on the observational data, the models, and the forecaster experience.

On a global scale, the International Space Environment Service (ISES, <http://www.spaceweather.org>) provides daily space weather monitoring and forecasting and brings together space weather monitoring centers from 19 countries around the world. This organization is the main international body devoted to the promotion of such services, facilitating the exchange of data and the exchange between those centers of best practices in providing space weather services. The NOAA Space Weather Prediction Service (SWPC) in the USA is the best-known member. In Europe, space weather services are offered among others through the ISES Regional Warning Centers in the UK (MetOffice), Belgium (Royal Observatory of Belgium), and Poland (Space Research Center). In Europe, the European Space Agency (ESA) has federated many European space weather assets in its Space Situational Awareness (SSA) network with specialized entities (the Expert Service Centers) explicitly focusing on a specific physical domain. The ESA/SSA network concept is still in development and is to be considered preoperational.

The need for globally coordinated observations has recently been channeled through the World Meteorological Organization where a dedicated work stream (Inter-Programme Team on Space Weather Information, Systems and Services) is in the process of including the corresponding observation requirements within the WMO databases regarding observation requirements.

### **Specific Defense Challenges**

Space is sometimes considered the fifth warfare domain. It is at least a critical enabler for land, air, maritime, and cyber operations. Governments and armed forces strongly rely on space-based capabilities and services to fulfill their missions, especially in the frame of expeditionary and intelligence operations. Satellite communications, Global Navigation Satellite Systems (GNSSs), space-based Intelligence, Surveillance and Reconnaissance (ISR), and environmental monitoring are paramount for the success of operations. Therefore, timely reliable space weather information is essential.

The defense sector may be impacted by space weather effects on different levels. At the first level, one might expect military technology to be affected by space weather effects much like the civilian technology as discussed above. Obviously, details of the vulnerabilities of military technology are not readily available to space weather researchers. Here we discuss additional challenges faced by the defense sector beyond the direct impact on technology.

The first specific defense-related challenge is the relation between the needs for space weather services by military users and the capabilities and governance of currently developed space weather service systems. These space weather service systems are currently being developed out from the research community. Consequently, space weather warnings and alerts are typically formulated in scientific jargon describing the state of solar-terrestrial system as a physical system. Such information is not directly actionable by a military user in the field but needs to be translated in terms of potential impact on specific equipment. As this translation requires knowledge of the military equipment in use, it must be done by experts within the defense sector itself. These technical experts need to be trained to understand the scientific jargon and to be able to translate it into actionable information.

In this perspective, we notice huge disparities between the NATO Nations. In fact, only few NATO Nations are quite advanced while the majority has recently envisaged to bridge civil space weather services to the needs by military users. In America, the USAF (US Air Force) already works for years in close collaboration with the Space Weather Prediction Center (NOAA) and fully relies on its experience and knowledge in solar science to produce space weather forecasts. In Europe, the UK Met Office produces space weather forecasts for national civilian and military customers. Also, the Joint Meteorological Group (JMG) relies on the Solar and Terrestrial Center of Excellence (STCE) of Belgium for the provision of space weather data and has developed its own "Space Weather Impact Matrix" depicting the impact of space weather events on Dutch weapon systems.

In NATO, space weather has been recognized a specific matter and belongs to the METOC (Meteorological and Oceanographic) field of expertise. The United States is currently assuming the role of "Assisting Nation" (AN) for space weather. Last year, an ad hoc group has been created to work on standardization and harmonizing in the field of the space weather support to NATO operations.

In Belgium, the Meteo Wing of the Belgian Air Force (BAF) has started a collaboration with the STCE, especially in the field of education and training. What space weather products are concerned, the BAF currently relies on the US being the Space Weather AN. Nonetheless, the BAF strongly envisages extending its collaboration with STCE through the development of specific space weather products to support Belgian military assets and the support of the STCE in distributing and validating space weather advisories for the ICAO.

Another specific defense challenge is to distinguish a space weather impact from sabotage or jamming from the enemy. The same space weather source can affect a wide range of different technologies all over the planet. As we have discussed above, the impact includes reduction in communication possibilities, deterioration of positioning services, and unexpected malfunctioning. Confusion with a coordinated sabotage activity is therefore not excluded. In order to distinguish between a space

weather impact or deliberate action, it is necessary to maintain an awareness of the state of space weather.

As mentioned, the – mostly – civilian space weather systems are currently being developed by the research community, although armed forces throughout the world are becoming increasingly active in the field of space weather, for instance, the USA and the UK. This implies that much of the existing space weather services are dependent on research observational infrastructure, both on the ground and in space. This observational infrastructure typically has poor long-term perspectives, very little redundancy and security measures, and even its own functioning might be strongly affected when strong space weather occurs. An independent, fully operational infrastructure for space weather observations is required to maintain serious “space situational awareness.” This would involve many ground-based observatories (per time zone, redundancy for weather conditions) and/or many satellite observatories (remote sensing of the Sun from different perspectives, as well as in situ solar wind observations) and becomes therefore quickly prohibitively expensive for both civilian and military programs.

A final specific challenge for defense is at the extreme side of space weather events. Such extreme events have been observed in the past (e.g. 1859) but not in modern times when society has become fully dependent on power grids and satellite communication. The most extreme space weather events have the potential to damage the major transformers of the power grid worldwide (Schrijver et al. 2014). Such large-scale damage would require months to years for repair resulting in serious problems for basic services such as hospitals and water and food distribution and might ultimately lead to collapse of the civilian society. The original space weather driver of such unrest will have faded away in at most a few weeks but the military might be called upon to maintain homeland security for much longer.

---

## Conclusion

Space weather as driven by the variable activity of our nearby star, the Sun, has been around since before the dawn of humankind. Our increasing dependence on technology in space and on the ground makes us however increasingly vulnerable to the impact of space weather on technological systems. Whereas – in most sectors – everyday space weather can be handled through improved system hardening, the catastrophic impact that seldom but extreme space weather events can have, cannot be fully excluded. Given its dependence on global communications, accurate GNSS positioning, and satellite operations, also the defense and security sector must take the space weather risks into account. In this chapter, we have listed several historical space weather events that have had surprising impacts on military operations. We advocate that maintaining a “space situational awareness” requires structural communications between space physicists providing real-time analysis of the space phenomena, with technology expert operators that can estimate the impact of these phenomena on the technological systems that the end user cares about.

**Acknowledgments** The contribution by Capt d’Avi Damien Lebrun (Meteo Wing, Be) to section 4.3 is much appreciated.

## References

- Bieber JW, Clem J, Evenson P et al (2005) Largest GLE in half a century: neutron monitor observations of the January 20, 2005 event. In: Sripathi Acharya B, Gupta S, Jagadeesan P, Jain A, Karthikeyan S, Morris S, Tonwar S (eds) Proceedings of the 29th international cosmic ray conference, August 3–10, 2005, Pune, India, vol 1. Tata Institute of Fundamental Research, Mumbai, p 237
- Cliver EW, Svalgaard L (2004) The 1859 solar-terrestrial disturbance and the current limits of extreme space weather activity. *Sol Phys* 224(1–2):407–422. <https://doi.org/10.1007/s11207-005-4980-z>
- Cucinotta FA, Hu S, Schwadron NA et al (2010) Space radiation risk limits and Earth-Moon-Mars environmental models. *Space Weather* 8: S00E09. <https://doi.org/10.1029/2010SW000572>
- Eastwood JP, Biffis E, Hapgood MA et al (2017) The economic impact of space weather: where do we stand? *Risk Anal* 37(2):206–218. <https://doi.org/10.1111/risa.12765>
- Kelly MA, Comberiate JM, Miller ES et al (2014) Progress toward forecasting of space weather effects on UHF SATCOM after Operation Anaconda. *Space Weather* 12(10):601–611. <https://doi.org/10.1002/2014SW001081>
- Knipp DJ, Ramsay AC, Beard ED et al (2016) The May 1967 great storm and radio disruption event: extreme space weather and extraordinary responses. *Space Weather* 14(9):614–633. <https://doi.org/10.1002/2016SW001423>
- Knipp DJ, Fraser BJ, Shea MA et al (2018) On the little-known consequences of the 4 August 1972 ultra-fast coronal mass ejecta: facts, commentary, and call to action. *Space Weather* 16(11):1635–1643. <https://doi.org/10.1029/2018SW002024>
- Love JJ, Coïsson P (2016) The geomagnetic blitz of September 1941. *Eos* 97. <https://doi.org/10.1029/2016EO059319>
- Redmon RJ, Seaton DB, Steenburgh R et al (2018) September 2017's geoeffective space weather and impacts to Caribbean radio communications during hurricane response. *Space Weather* 16(9):1190–1201. <https://doi.org/10.1029/2018SW001897>
- Riley P (2012) On the probability of occurrence of extreme space weather events. *Space Weather* 10(2):S02012. <https://doi.org/10.1029/2011SW000734>
- Schrijver CJ, Dobbins R, Murtagh W, Petrinc SM (2014) Assessing the impact of space weather on the electric power grid based on insurance claims for industrial electrical equipment. *Space Weather* 12(7):487–498. <https://doi.org/10.1002/2014SW001066>

## Further Reading

- Large Solar Event Detected During Irma. NCEI/NOAA, 14 September 2017. <https://www.ncei.noaa.gov/news/large-solar-event-detected-during-irma>
- Missing British Sub Feared Lost, Safe; Search Called Off. *Amsterdam Evening Recorder*. LXXVII (158). Amsterdam, New York. 24 February 1956. p 1. [https://en.wikipedia.org/wiki/HMS\\_Acheron\\_\(P411\)#cite\\_note-4](https://en.wikipedia.org/wiki/HMS_Acheron_(P411)#cite_note-4)
- Odenwald S (2015) Solar storms: 2000 years of human calamity. CreateSpace Independent Publishing Platform. ISBN-10: 1505941466



# Space Security in the Context of Cosmic Hazards and Planetary Defense

# 53

Joe Pelton

## Contents

Introduction .....	1026
Cosmic Hazards from Potentially Hazardous Asteroids and Comets .....	1029
Protective Strategies for Planetary Defense Against Asteroids and Comets .....	1033
Solar Weather and Ionic Storms that Threaten Planet Earth .....	1034
Solar Shields and Other Planetary Defense Strategies .....	1037
The Complication of the Earth's Shifting Magnetosphere .....	1039
Conclusions and Strategies for the Future .....	1040
References .....	1041

## Abstract

When most people think of space security, and especially “space safety,” they tend to think of space safety for astronauts and successful launch of satellites, or strategic systems related to missile defense. Some may even think of the threats that could come from orbital space debris. This chapter, however, examines space security from yet another perspective. It addresses cosmic hazards that humanity faces from asteroids, comets, solar storms, and even shifts in the Earth magnetosphere. These space hazards are very real threats to global security and modern civilization. Too often we tend to forget that our world travels through the hostile environment of outer space and is indeed quite vulnerable to cosmic hazards of various types.

This chapter focuses on the fact that humans live on a six sextillion ton planet that orbits the sun once a year and travels millions of kilometers through a quite dangerous cosmic environment as it speeds through space at close to 100,000 km/h.

---

J. Pelton (✉)

International Association for the Advancement of Space Safety (IAASS), Arlington, VA, USA

e-mail: [joepelton@verizon.net](mailto:joepelton@verizon.net)



Chapter 11 in Part 1 of the HOSS discusses “space safety” from the perspective of astronaut and spacecraft risk and reliability, and also considers the problems of sustainability of space, orbital debris, and space traffic management.

This chapter, however, addresses “space safety” from the perspective of asteroids and comets that are potentially hazardous and could impact Earth in various ways – in the air, on land, in the oceans, or just offshore. It also addresses the hazards that come with solar storms that include high-energy X-ray flares and coronal mass ejections (CMEs). Further the chapter even addresses emerging problems associated with the Earth’s reversing magnetic poles. The now clearly detected shift in the geomagnetosphere is a concern. This is because during this time of reversal, the Earth’s natural protective shielding against the ions from the sun that come with CMEs are greatly diminished. This means that humanity and our electrical power grids, pipelines, communications networks, and satellites will be much more vulnerable to violent solar storms during the time of this magnetic reversal.

The structure of this chapter is that it first addresses the threat to the world from potentially hazardous asteroids and comets. It then addresses the issue of solar radiation flares and coronal mass ejections (CMEs), and then finally it addresses the complication that comes from the reversal of the Earth’s magnetic north and south poles.

---

### Keywords

Anthropocene Age · Comets · Coronal mass ejection (CME) · European Space Agency · Geomagnetosphere · International Asteroid Warning Network (IAWN) · Mass extinctions · NASA · National Atmospheric and Oceanic Administration (NOAA) · Near-Earth objects · Potentially hazardous asteroids · Solar flares · Solar storms · Space Mission Planning Advisory Group (SMPAG) · Space weather · UN Office of Outer Space Affairs · UN Committee on the Peaceful Uses of Outer Space · Van Allen Belts · X-Ray flares

---

## Introduction

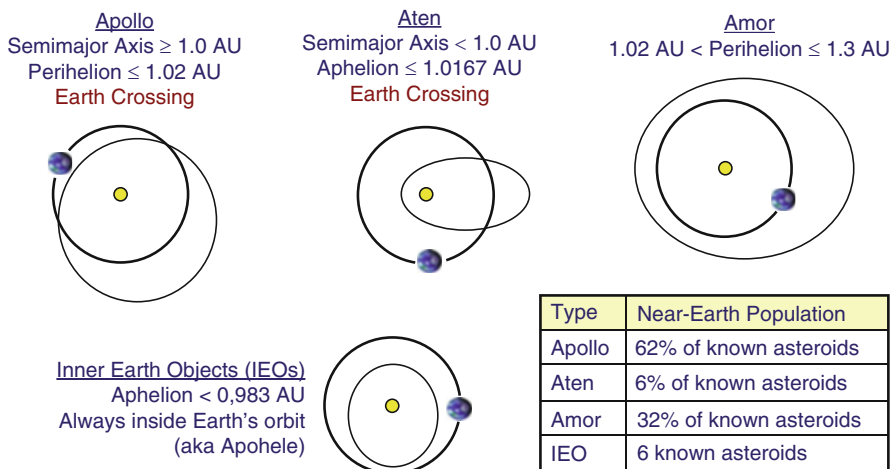
The dinosaurs that were wiped out by the so-called K-T Mass Extinction some 65 million years ago really never knew what hit them. The Earth’s various plant and animal life forms have to date experienced five mass extinctions that have each occurred hundreds of millions of years apart. Four of these event have come from thermal shifts in the Earth’s atmosphere, but the most recent one, the K-T event, came when a 5-km-wide asteroid crashed into the coast of Mexico and the Caribbean Sea and created a massive cloud that blocked out the sun, killed off the dinosaurs and three-fourths of all species on Earth, and led to the rise of mammalian life forms over the life forms that became extinct (The K-T Mass [2018](#)).

And killer asteroids are not safely things of the past. In May 2018, two potentially hazardous asteroids, one the size of a city block zoomed by Earth within the lunar orbit. Indeed the largest one passed only 114,000 km away (Close Encounter [2018](#)).

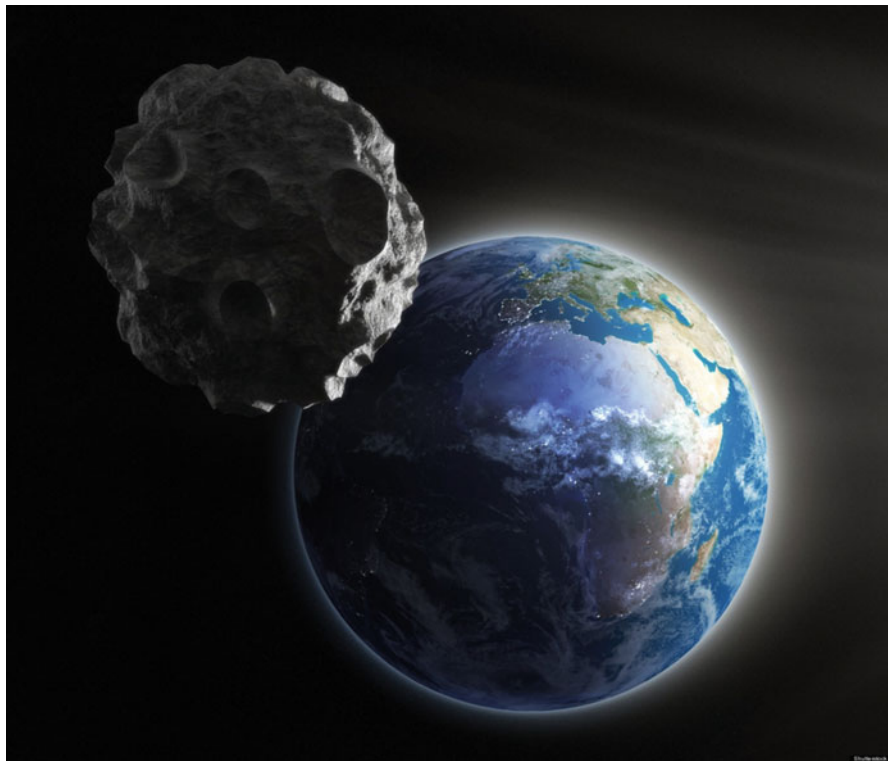
In February 2018, a smaller asteroid came within 70,000 km of smashing into our world (Bob King 2018). In cosmic dimensions, these “near misses” are considered uncomfortably close. Although the millions of asteroids in our solar system are largely concentrated in the asteroid belt, there are perhaps tens of thousands of asteroids that are close enough and large enough and travelling fast enough that they are of a serious concern. The potentially hazardous asteroids that are tracked by ground observatories or infrared space telescopes are generally grouped into four categories. These are pictured in the graphic below. The most common are Apollo (representing some 62% of the inventory) and Amor (representing 32% of the inventory). The other types are characterized as Aten (representing some 6%) and finally Atras which are the Inner Earth Objects (IEOs). Atras, which are the least common, currently represents a total population of only six potentially hazardous asteroids. Recently, a Trojan asteroid that follows the same orbit as Earth around the Sun has been located to create yet another category (See Fig. 1) (Jet Propulsion Laboratories 2018).

There is a concerted worldwide effort to detect and track potentially hazardous asteroids. These near-Earth asteroids (NEAs) and/or near-Earth objects (NEOs), also known as potentially hazardous asteroids (PHAs) are of special concern. NEA or PHAs are defined as those objects whose orbits come within 0.05 astronomical units (or 7.5 million kilometers) of our planet and have a magnitude (H) of 22 or brighter. When an asteroid actually impacts Earth, its mass and velocity can do great damage (See Fig. 2).

And unfriendly asteroids are not the only cosmic hazard that threaten our planet. In 1859, the so-called Carrington event, a coronal mass ejection from the Sun, bombarded Earth with trillions of high-speed ions. This led to telegraph offices catching on fire and the “Northern Lights” descending all the way done to Cuba and



**Fig. 1** The types and population frequency of potentially hazardous asteroids. (Graphic courtesy of the Jet Propulsion Labs)



**Fig. 2** Potentially hazardous asteroids streak past Earth with regularity. (Graphic courtesy of NASA)

Hawaii. Records in China suggest that a similar solar storm event occurred in the early 1700s. More recently, there was the 1989 Montreal event that wiped out many transformers from Chicago to Montreal. In 2003, there was the Halloween event that impacted the electrical grids in Scandinavia. In areas exposed by the so-called Ozone holes in the polar regions, there are also particular concerns with solar flares represented by high-energy x-rays and ultraviolet radiation. These flashes of radiation, if not blocked by the Ozone layer of Earth's atmosphere, can expose animals and people to genetic mutation and elevated risk of skin cancer. Any serious examination of space security and "space safety," must therefore consider the risks that come from cosmic hazards and consider the extent to which today's and tomorrow's space programs could mitigate these risks through the use of space systems and technology either today or in the future. We are now beginning to develop new and sophisticated space systems and technology that could protect our small and fragile planet against such cosmic hazards.

It is ironic that as we develop new types of space systems that could protect Earth from these cosmic hazards, that there are real threats to humanity originating here on Earth. The exponential growth of global human population, the spread of industrial

pollution, and other types of human activities are now beginning to threaten the world's biosphere via climate change and over consumption of the Earth's limited resources. This growth of the human impact on our planet has led geologists to proclaim that we now live in the Anthropocene Age. This means that human activity is the major shaper of the world's geology and ecology. Some suggest that these trends might even lead to what might be called the "Sixth Mass Extinction" or "Anthropocene Mass Extinction." Apparently, today's world needs protection from both cosmic hazards as well as human expansionist trends and climate change here on Earth (Mooney and Dennis 2018).

Today the risk that comes from potentially hazardous asteroids or comets is now quite severe. This is because of potential loss of life, devastation to vital infrastructure, and environmental impacts that could occur. Yet, although the risk of devastation is large, the probability of a near-term collision is thought to be remote. Indeed, the probability is much higher of Earth being hit by a deadly solar storm that could disrupt the lives of a huge number of people in modern society. Indeed, it is far more likely that a massive coronal mass ejection (or solar storm) could provide major disruptions to our modern infrastructure of electrical power systems, pipelines, satellites, and industrial control systems on which we now greatly depend. If we picture Earth as an apple, then our atmosphere that protect us would be represented by the skin of the apple. Today there is a wide range of activities with regard to sustainability of space, defense of Earth against asteroids and comets via the International Asteroids Warning Network (IAWN) and the Space Mission Planning Advisory Group (SMPAG), and activities related to research and protective programs related to extreme space weather events and the Earth's magnetic fields. It is not possible to list all of these activities in a comprehensive manner in this one article. Even if an attempt were made, the listing would be soon out of date. It is recommended that the UN Office of Outer Space Affairs website be consulted to obtain useful updated information by visiting the following and related websites: [http://www.unoosa.org/documents/pdf/smpag/st\\_space\\_073E.pdf](http://www.unoosa.org/documents/pdf/smpag/st_space_073E.pdf)

---

## **Cosmic Hazards from Potentially Hazardous Asteroids and Comets**

The threat, or risk level, from potentially hazardous asteroids is not easily assessed. When NASA was first asked by the U.S. Congress about the cosmic hazards there was difficulty finding a good answer as to the extent of the planetary threat level. NASA first suggested that a comprehensive inventory of asteroids that could threaten Earth might be set at 1 km in diameter. In subsequent discussions with Congress with NASA, it became clear that 1 km was not sufficient. When the George Brown Act part of the NASA Authorization Bill was passed in 1993, it was agreed to refine the research parameters. Thus they reduced the size of PHAs for the NASA search inventory for threatening asteroids to 140 m or larger. NASA, under this legislation, was to have completed this inventory with a comprehensive list of all such PHAs by now but still have not been able to finish this search process. Although over 90% of PHAs over 1 km in size have been identified, the inventory of asteroids

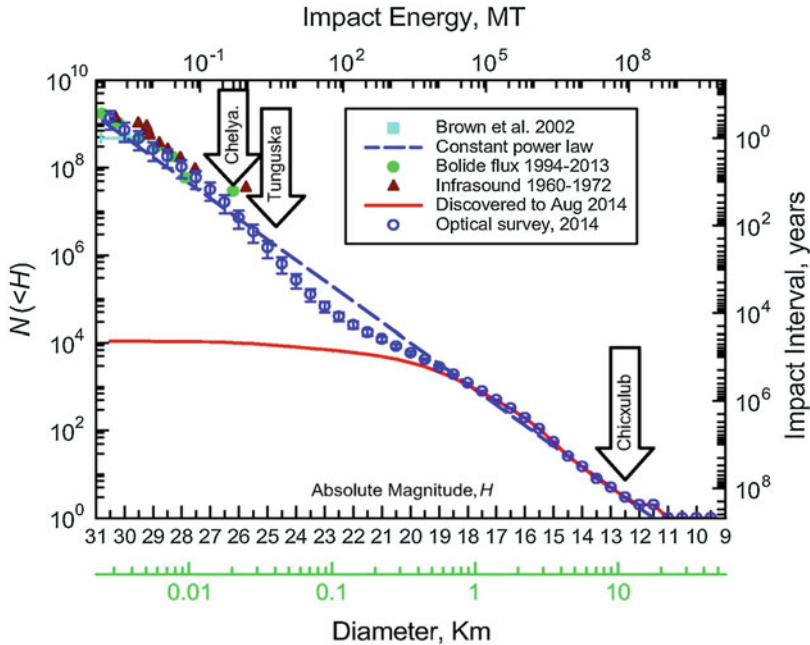
down to 140 m is still far from complete. The NASA NEOWISE program has helped to identify numerous NEAs, but this infrared space telescope program has now finished its mission. NASA has plans for a new infrared telescope to assist with this discovery process, called NEOCAM, but it is still in a Phase 1 definition and would not be launched before 2022 or 2023 (Maizer et al. 2015). Based on a so-called “de-biased” sampling of the results achieved with the NEOWISE asteroid search program, it was estimated that only 25% of asteroids greater than 100 m have now been identified. The estimate as to the likely this unidentified population of potentially hazardous asteroids above 100 m in size is estimated to be somewhere between 3200 and 6200 (or 4700 plus or minus some 1500) (Ibid.). This is a rather frightening number when it is realized that 35 m asteroids could be “city killers” and that the estimated number of unidentified PHAs of this size could possibly be in the tens of thousands.

The problem is that the experience that comes with the study of past asteroid strikes such as the Tunguska strike in Siberia, Russia, in 1908 (estimated to be some 40 m in diameter) that asteroids that are only 30–40 m in diameter could destroy an entire city anywhere on Earth. Indeed the area of devastation from the Tunguska strike covered an area equivalent to the size of the San Francisco Bay area. There have been others that such as the B612 Foundation that has suggested that an infrared space telescope could be designed with the discriminatory capability to detect potentially hazardous asteroid down to 35 m in size. This project that was called Sentinel would be designed to detect “city killers” that could still create massive destruction should it actually make a direct hit on a major city. In short, it would be able to detect many more PHAs and of much smaller size than NASA’s intended infrared space telescope that is designed to meet the 140 m radius standard officially set by the U.S. Congress.

Figure 3 shows in details the relationship between the diameter of asteroids, their typical kinetic energy, their numbers (or frequency of their occurrence), and the likelihood of their hitting Earth. Specific examples of major asteroid strikes that occurred in the past are noted in the case of Chelyabinsk, Russia, that impacted with an energy level of about 100,000 tons of TNT and the case of Tunguska, Russia, that impacted with an impact energy level of about 1 megatons of TNT.

This type of chart suggests that large asteroid or large meteor strikes impact with great energy, but that such impacts are fortunately also rare. Indeed this is not only because larger asteroids are fewer in number but also because we are also, in a sense, protected. The enormous gravitational fields of the Sun and the Jupiter are far more likely to scoop up such large space rocks before they crash into Earth. The unfortunately part of the equation is that there are so many asteroids and even comets out there. Many millions are safely in the asteroid belt, yet there are still tens of thousands of potentially “city killing” asteroids that could still hit Earth and release terawatts of kinetic power as they crash into earth with the force of a nuclear explosion (Pelton 2015).

It is important to note that the number of asteroids of a larger size are exponentially less in number. Alternatively, this means that as the size of asteroids decreases, the number of them increases exponentially. Larger and therefore more deadly



**Fig. 3** Different sizes of near-Earth asteroids and impact energy in equivalent megatons of TNT. (Chart courtesy of NASA)

asteroids, as well as comets, which travel at even more deadly speeds, are fortunately likely to be captured by other bodies in the Solar System such as the Sun or Jupiter since these objects have much greater gravity wells than Earth. But what might be misleading is that the frequency of occurrence does not mean that the next deadly asteroid strike can be counted on to be thousands or even millions of years in the future. In truth, a major strike could threaten within the next year. Further the projected deaths shown in Table 1 are not truly foreseeable since it would depend on where and how it landed. If the 44 m asteroid indicated in the chart landed in a totally isolated area, such as Tunguska, it might result in no deaths, but if it landed directly on Moscow, New York, London, Beijing, or Mexico City, then the deaths could be in the many thousands or even millions. As the Earth becomes more populated and the number of megacities with a population of 10 million or more continues to rise, the risk of a catastrophic impact from an asteroid also rises. (See Table 1)

The other possibility, of course, is a comet impact. Comets that could threaten Earth are fortunately much rarer than potentially hazardous asteroids. The speed and size of comets could make their impact far more devastating. The Shoemaker-Levy comet cluster impacted Jupiter in giant pieces up to 2 km size between 16 and 22, July 1994. Each of these pieces of the comet, which were traveling at speeds of about 60 km/s, could have created incredible damage if they had smashed into Earth and threatened the existence of all living things on our planet including humanity.

**Table 1** Key estimated impact figures for potentially hazardous asteroid

Asteroid damage parameters						
Ground impact	Probability/year	Diameter	Blast radius	Deaths	Ground damage	Interval within Lunar Orbit (i.e., within 400,000 km)
<b>5 megaton event</b>	$1.67E^{-03}$	<b>44 m</b>	<b>About 20 km</b>	<b>About 200</b>	About 1200 km <sup>2</sup>	1/20 years
<b>100 megatons</b>	$1.00E^{-04}$	<b>120 m</b>	<b>About 60 km</b>	<b>About 19,500</b>	About 10,000 km <sup>2</sup>	1/80 years
<b>1000 gigatons</b>	$2.00E^{-06}$	<b>3 km</b>	<b>About 500 km</b>	<b>Unknown</b>	About 800,000 km <sup>2</sup>	1/600 years

Note: Figures are estimates that would vary significantly depending on actual point of contact

Currently, there are efforts to address the threat of Earth being hit by either an asteroid or comet in future years. The U.N. General Assembly has sanctioned the creation of the an International Asteroid Warning Network (IAWN) whose work is coordinated by the U.N.'s Office of Outer Space Affairs ([International Asteroid Warning Network](#)).

The Minor Planet Center in Cambridge Massachusetts plays a key role in cataloging all of the near-Earth asteroids as reported by infrared space telescopes and by at least 30 ground observatories and space-based infrared telescopes (The International Astronomical Union (IAU) Minor Planet Center 2018). A listing of the 30 ground-based observatories and their asteroid discoveries can be found at the following website ([List of Asteroid-Discovering Observatories](#)). The greatest number of asteroids in recent years has come from the NEOWISE (Near Earth Orbit Wide-range Infrared Surveyor Explorer). This IR Space Telescope during the period of its reactivation between 2013 and 2016 discovered 541 NEOs and 99 comets (Howell 2016). This capability will in theory ultimately be replaced by the NASA NEOCam mission. Currently, during the Phase A study authorized in January 2017 will consists of an infrared telescope and a wide-field camera operating at thermal infrared wavelengths. The NEOCam telescope has been funded for an extended Phase A study by NASA in the Planetary Defense Coordination Office will, however, be limited under current guidelines to searching for asteroids of a size of only 140 m and larger (NEOCam 2018).

This worldwide effort is also assisted by the Spaceguard Foundation in Italy (The Spaceguard Central Node 2018), The International Astronomical Union (IAU), the International Academy of Astronautics (IAA), the Spaceguard Foundation, the various national and regional space agencies, plus nongovernmental such as the Planetary Society, the B612 Foundation, and the Secure World Foundations (SWF) are all very much involved in considering how to better identify threats from near Earth objects (NEOS). Scientific bodies and NGOs have for instance suggested that search strategies should be seeking to identify asteroids that are smaller than 140 m in size and promoted the idea of launching new infrared space telescopes

that are able to identify NEOs that are as small as 35 m in diameter. Indeed the B612 Foundation has defined such a space mission, named Sentinel with an estimated cost of \$450 million that could find NEAs down to this size. When NASA ended matching funding in 2015, the B612 Foundation end this program and is now exploring a smaller constellation of small sats that might be able to complete an inventory of threatening asteroids of smaller size (B612 2017).

When the U.N. General Assembly in 2013 sanctioned the creation of the IAWN, they also sanctioned the creation of the Space Mission Planning Advisory Group (SMPAG) to address strategies and even actual missions to address identified cosmic threats. The work of the IAWN and the SMPAG are both overseen by the U.N. Office of Outer Space Affairs (OOSA). The responsibility of the IAWN is to create an international warning network to identify the threat. The responsibility of the SMPAG would be to consider actual strategies that might be employed to ward off an asteroid or comet that might threaten a direct impact with Earth in the future (UN Asteroid Defense Plan 2013). It is recommended that one visit the website of the U.N. Office of Outer Space Affairs to learn more about the most recent activities in these areas.

---

## Protective Strategies for Planetary Defense Against Asteroids and Comets

There have been a wide range of possible strategies that have been discussed to address what to do if a definitive threat to Earth by an asteroid or comet is identified. These strategies have varied from longer term strategies that are consistent with years of advance warning. These activities might include such efforts as undertaking the deployment of so-called “Laser Bees.” This would be a small sat mission where lasers activated from small sats would create small jet streams of ejected mass from asteroids so as to divert the asteroid’s path (Laser Bee Project 2014). There are other concepts that have been identified that involve placing a satellite of some mass in close proximity to the threatening NEO so that its gravitational effects (i.e., to become a “gravity tractor”) would over time move the NEO into a less threatening orbit (Sohn 2018). These strategies would likely be more suited to an asteroid than a very fast moving comet.

Another type strategy might involve either a kinetic impact between a spacecraft – perhaps equipped with a bomb – and a PHA in order to divert its path. This also might be done via a particle beam system that would create momentum transfer to divert the asteroid’s path. One version of this approach would be for enterprises engaged in “space mining” to engage in a “two-fer.” Thus they would divert a NEO into Lunar orbit so as to extract resources from the asteroid over time. They would, however, equip the asteroid with thrusters that would allow a collision between the threatening asteroid and the “mined asteroid” in lunar orbit so as to prevent either space object colliding with Earth.

There are other versions of such shorter-term strategies. This might including creating a directed high energy beam to blast the PHA long enough to divert its path.



Or, as has been depicted in films, there might be a mission to an asteroid in order to detonate a bomb or even nuclear device to blow the asteroid apart. There are currently various types of research programs around the world to better understand the composition and shape of asteroids and to examine which of these strategies would be most effective and which might be best used with longer, medium, or short-term warning of the threat (Atkinson 2011).

There are efforts such as the European Union-led NeoShield initiative. But such efforts are today only modestly funded by a few millions of dollars. Only a truly well-funded program involving billions of dollars could develop the needed capabilities – especially for short reaction time programs (<http://www.neoshield.eu/neoshield1-summary/neoshield-1-team/>).

There have been nearly 10,000 NEOs identified. NASA has currently identified some 1400 asteroids that are considered the most serious threats as potentially hazardous asteroids that are plus 1 or plus 2 on the Palermo Threat Scale. Some asteroids are projected to be in orbits that could come quite close to Earth in the next few years. Aphopis, for instance, is now being tracked in an orbit that will come dangerously close in 2029 and 2036, but it is not expected to actually hit Earth in those years. Some have suggested that there are large asteroids concealed in the Taurid Meteor Shower that is associated with Comet 2P/Encke, and others suggest that a better inventory is needed of all the periodic meteor showers that bombard Earth during yearly cycles to determine there are not deadly space rocks concealed in these meteor clouds.

The thing that is most clearly true is that the inventory of potentially hazardous asteroids is still far from complete and that an accounting of asteroids that is limited to those that are larger than a 140 m threshold is inadequate. The second conclusion that is not as clear. We should seek to develop planetary defenses against comets and asteroids. But it is unclear as to what systems or technology can create the best space guards against cosmic hazards. We still do not know what are the most effective and cost-efficient strategies that might be used to defend Earth against impending threats from a near Earth asteroid or comet? Although the UN-sanctioned International Asteroid Warning Network (IAWN) and the Space Mission Planning Advisory Group (SMPAG) are a start, we are still a long way from knowing exactly what and how to defend Earth against such hazards and who should be in charge of such activities.

---

## **Solar Weather and Ionic Storms that Threaten Planet Earth**

The two main cosmic threats differ greatly in terms of their frequency of occurrence. During solar max in the 11-year cycle of solar activity, there can be several coronal mass ejections a day and solar radiation flares are twice as common as the ionic blasts. In short, solar storms of significance are much more common than major strikes by asteroids or comets. Yet large cosmic bodies slamming into Earth will typically do much more damage. The bottom line, however, is that asteroids, comets, solar radiation flares, or coronal mass ejections can all do significant harm. A major

coronal mass ejection that creates major problems, such as the so-called Carrington Event of 1859 are projected to occur every 150 years while a major devastating asteroid hit seems to space millions of years apart. The difficulty is that “average frequency of occurrence” does not mean that a catastrophic event might not occur tomorrow. The concern level as to a major coronal mass ejection strike should be high for several reasons: (i) It has been some 160 years since the last truly major coronal mass ejection; (ii) the only truly significant result of the Carrington event of 1859 was telegraph offices catching on fire, but with today’s world, the risks are enormous in terms of possible adverse affects on electrical power grids, pipelines, industrial control systems, telecommunications and data networks, and satellites; (iii) the world’s population since 1859 has grown from 1.5 billion to some 7.5 billion and that population is 53% concentrated in urban centers hugely dependent on modern lines of supply and service-based jobs that are heavily dependent on electrical power grids, telecommunications and data networks, pipelines, satellite systems, and other infrastructure vulnerable to a CME containing trillions of ions blasting Earth with incredible force.

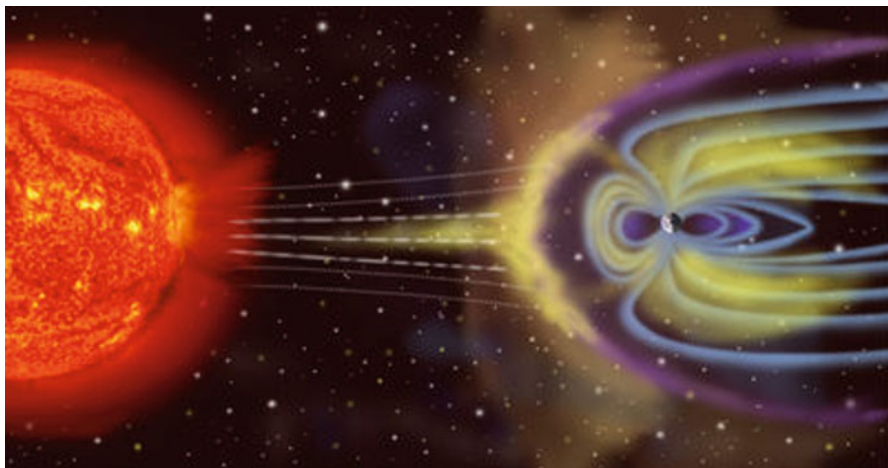
There is a constant stream of so-called solar wind that streams from the sun but typically this “normal” space weather is warded off by the Earth’s geomagnetosphere with little or no affect on our daily lives.

During Solar max, there are perhaps 10–12 X-Class (or the very highest energy X-ray emissions) solar flares and about half the time these will be accompanied with tremendously powerful coronal mass ejections that send trillions of ions at millions of kilometers/hr outward from the sun. About ever dozen years there is an EMP that will reach Earth and do damage to electrical power grids and information networks. The Montreal event of 1989 and the Scandavian Halloween event of 2003 represent examples. Fried electrical transformers are the most common result of such an event, but many types of infrastructure on Earth, in the skies, and in orbit are potentially at risk (See Fig. 4).

The smashing into the Earth’s electromagnetic shields by high energy ions traveling at millions of kilometers/hour is a tremendously disruptive force that stresses the magnetic fields so they stretched over 30 times the Earth’s diameter before they resume their normal form that are seen in the usual shaping of the Van Allen belts. Without this protective shielding, Earth would not have its life-giving atmosphere.

Mars, which lacks an iron core such as that possessed by Earth, does not have a magnetic field to protect it. The solar wind thus continually strips away Mars’ atmosphere. Then coronal mass ejections blasts away virtually all of the modest atmosphere that Mars’ gravity manages to maintain. Thus Mars is only able to sustain about 60 milli-bars of atmospheric pressure.

When solar wind reaches Earth, the magnetic field pushes off the solar ions to the North and South Poles and it is this solar phenomena that create the aurorae that can be seen there. Sometimes Earth’s location is called a “Goldilocks” planet since our world is just the right distance away from the Sun in terms of temperature and radiated light and its gravitational field is ideal for human physical characteristic. One should also note that its geomagnetic shielding is just right to sustain an



**Fig. 4** Depiction of a coronal mass ejection showing impact on Earth's magnetic fields. (Graphic courtesy of NASA. Note: Graphic is not to scale)

atmosphere that is able to sustain life and protect against harmful radiation and solar ions. The Earth's Van Allen Belts and ozone layer are critical to sustaining life in our "Goldilocks" world. Without this protective shielding, the radiation from the sun would create enormous problems due to skin cancer and genetic mutation would lead to birth defects and other problems.

The natural protections of our planet have been sufficient to sustain life and allow human civilization to develop for millions of years. The twenty-first century that has seen humanity to grow to unparalleled numbers that might reach 10–12 billion by 2100 and lead to 80% urbanization with heavy dependence on modern infrastructure could lead to a new level of vulnerability in many ways. Modern jobs and urban living are now dependent on electrical power systems, pipeline networks, telecommunications, data and transportation networks, and satellite systems. If solar storms could knock all of these systems out of operation, then billions of people could be put at risk in terms of having food to eat, jobs to support economic viability, and protection against genetic mutation. The unprecedented growth of humanity from 800 million in 1800, to 1.8 billion in 1900, to nearly 7 billion in 2000 now exposes humanity to risk due to over development, global warming and climate change, and major disruptions if modern infrastructure is somehow disabled (Pelton and Marshall 2010).

It is for the above reasons that the threat from solar storms should be taken quite seriously. Currently vital governmental units, such as the U.S. National Oceanic and Atmospheric Administration (NOAA), which is a part of the U.S. Department of Commerce, are providing a real-time monitoring capability of space weather. There is a web-based space weather dashboard that reports on many different aspects of space weather. There are special networks to providing warnings – especially with regard to X-Class solar radiation flares and high-energy coronal mass ejections

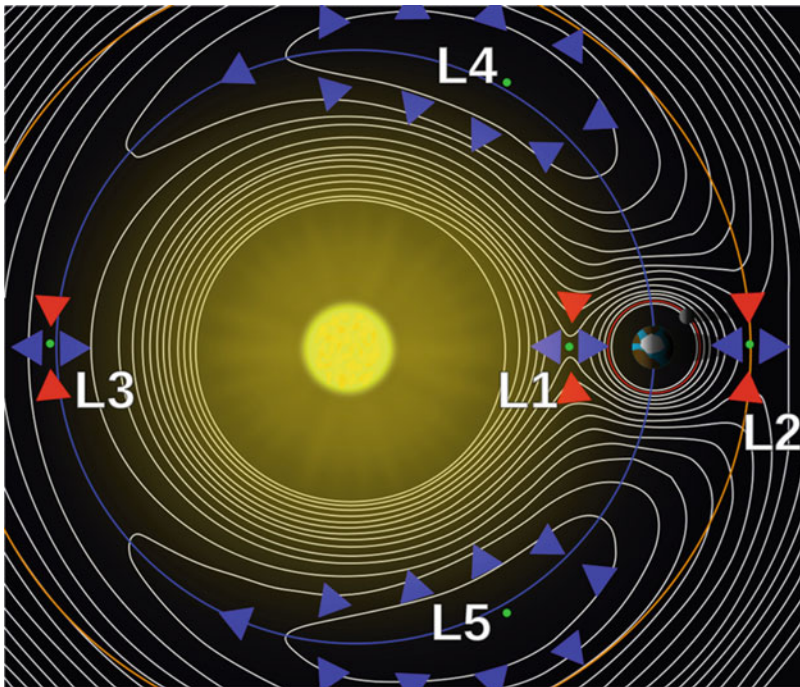
(CMEs) that could threaten everything from electrical power grids to everything that depends on electrical power to sustain their operation. Defense ministries have their own monitoring and alert systems as well.

These efforts are currently aimed to provide systems alerts. There are some efforts to create more robust protective circuit breaker systems and more accurate and rapid warning systems, but the next step to consider what form of protective shielding might be created in space to provide some form of shield against major solar storms is largely in the realm of science fiction. It is now time to recognize the extent of the danger that solar storms present to the global economy and to explore what types of protective steps might be taken.

---

## Solar Shields and Other Planetary Defense Strategies

The natural location to consider for a protective solar shield is clearly Lagrangean Point 1. This is the location about 1.5 million kilometers out in space – well beyond the Lunar orbit – where the gravitational field of Earth and that of the Sun are more or less in balance or a form of homeostasis. This is actually more of an “area” than a point as demonstrated in Fig. 5.



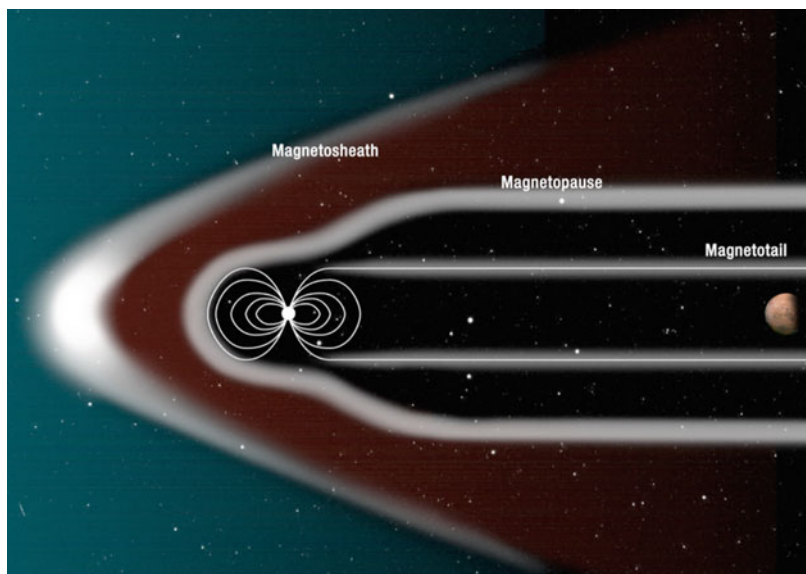
**Fig. 5** The Lagrange Point L1 where Earth and Sun gravitational fields balance. (Graphic Courtesy of NASA)

The key would be to create a large enough magnetic field, both in magnitude and geographic size such as 2–4 Teslas covering a 1000 km<sup>2</sup> such that a blast of CME ions would be diverted to the sides so that the ion stream would miss Earth and not “tail” around the space shield and come back together so as to still impact Earth.

The idea of creating a solar shield, sometimes called a LAPSE (LAgrange Protection for Solar Ejections), has two significant elements to consider. One element is that a LAPSE could be created not only for Earth but for Mars as well. Mars has no natural magnetic protection and accordingly has its atmosphere stripped away. A LAPSE for Mars has the potential to create a significant atmosphere that could sustain life in the future. The projections have been made to suggest that Mars atmospheric density could increase from 60 milli-bars to ten times this density over time (Green et al. 2017) (See Fig. 6).

The other element is that a Lagrange Point 1 (LP1) facility could be expanded to undertake additional function such as Solar System wide transit point with virtually no take-off gravitational limitations to reach any point of destination. Further this location would also be idea for creating a solar radiation modulation system that could provide some temporary limits to global warming due to climate change while longer term solutions are devised.

There is a particular reason why the idea of a LAPSE Solar Shield is a concept of some urgency to be considered and implemented for Earth as soon as it could be designed and implemented. This reason is the current reversal of the world’s magnetic poles. This reversal could weaken in a significant way the natural geomagnetic shield that Earth currently enjoys.



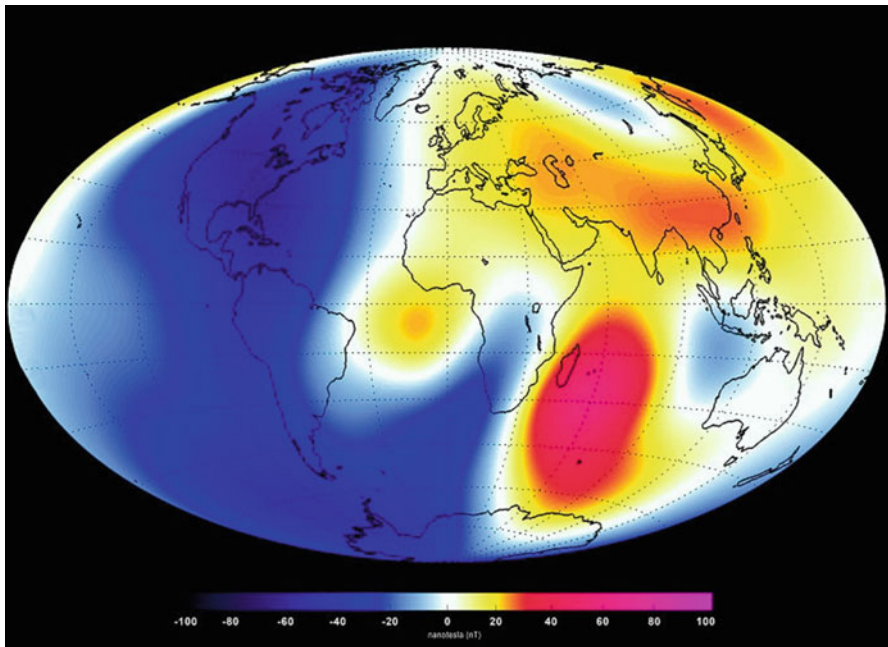
**Fig. 6** An artificial magnetosphere of sufficient size generated at L1 allows Mars to be well protected by the magnetotail. (Graphic courtesy of James Green, NASA)

## The Complication of the Earth's Shifting Magnetosphere

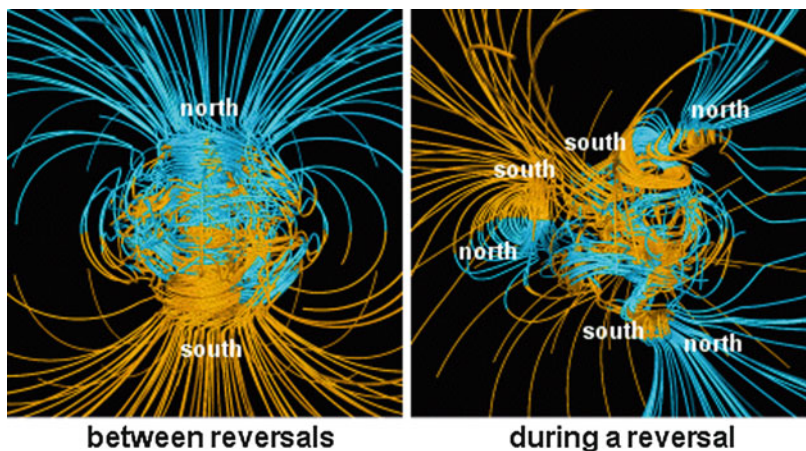
Currently, there are two satellite missions measuring the Earth's changing magnetosphere. One is operated by the European Space Agency and is a three-satellite constellation called Swarm. The other is the NASA mission that is called the Magnetospheric Multiscale (MMS) constellation of four satellites flying in tightly configured constellation. Both mission are confirming that the world magnetosphere is changing and that the Earth's magnetic poles are shifting. Figure 7 below shows this shifting magnetosphere and how magnetic North has moved down to Siberia and the magnetic South has traveled upward as well.

There is now evidence of an irregularity in the Earth's iron-based core under Africa may be responsible for this shift to occur over long spans of time (Pappas 2018). The timing of this shift is not known, nor is the impact of this shift on the natural protective shielding of Earth from coronal mass ejections. There has been some computer modeling that suggest that the future results could be quite daunting. Some modeling as shown in Fig. 8 suggest that the natural shielding could be reduced down to 15% of the current shielding as defined by the current conventional shaping of the Van Allen belts as shown in the right and the quite distorted shaping during the reversal process.

The future might be envisioned as a "perfect storm" of adverse factors. This future of expanding global population, higher levels of urbanization, greater



**Fig. 7** Survey of Earth's changing magnetosphere. (Graphic Courtesy of ESA)



**Fig. 8** Computer modeling of changes to the Earth's magnetic field during magnetic reversal

dependence on electrical power grids, telecommunications and data networks, industrial control systems, and satellites that are more and more vulnerable to solar storms as the magnetic poles shift and natural shielding is eroded more and more.

---

## Conclusions and Strategies for the Future

The twenty-first century world and human civilization is vulnerable to significant cosmic hazards. These include potentially hazardous asteroids, comets, solar flares, coronal mass ejections, and eroded natural shielding as the Earth's magnetic field reverses. There is a need for agile and innovative adjustment to these conditions by global policy makers. The space agencies of the world need to adjust their mission and priorities. Space exploration and missions to the Moon and Mars are worthwhile objectives, but if the viability of human survival race and vital infrastructure on which the world depends becomes clearly and unequivocally at risk, then innovative space design and construction projects such as solar shields, improved IR space telescope to identify asteroid and comet threats, and space systems to cope with NEO hazards.

Space security and safety is more than astronaut safety, missile defense, reliable satellites or coping with the hazards of orbital space debris. The world of space is on the edge of a new era where mega-construction projects in space are technically and intellectually possible. The key to such progress forward is perhaps first and foremost a clear vision and a setting of new priorities for space agencies for the next stage of the twenty-first century.

## References

- Atkinson N. Every way devised to deflect an asteroid. *Universe Today*, 9 Nov 2011. <https://www.universetoday.com/90798/every-way-devised-to-deflect-an-asteroid/>
- B612 studying smallsat missions to search for near Earth objects. *Space News*. 20 June 2017. <http://spacenews.com/b612-studying-smallsat-missions-to-search-for-near-earth-objects/>
- Close encounter: asteroid as big as a football field will whiz right by Earth this week. *Tribute*, 13 May 2018. <https://www.sanluisobispo.com/news/nation.world/world/article211064469.html#storylink=cpy>; <https://www.sanluisobispo.com/news/nation-world/world/article211064469.html>
- Green J et al (2017) A future mars environment for science and exorption. *Planetary Science Vision 2050 workshop*, (LPI contribution no. 1989)
- Howell E. WISE: NASA's infrared asteroid hunter. *Space.com*, 4 Aug 2016. <https://www.space.com/33659-wise-space-telescope.html>
- International Asteroid Warning Network. <http://iawn.net/about.shtml>
- Jet Propulsion Laboratories. <http://neo.jpl.nasa.gov/neo/groups.html>. Last accessed 6 Oct 2018
- King B. Asteroid 2018 CB Zips by Earth. *Sky and Telescope*, 7 Feb 2018. <https://www.skyandtelescope.com/astronomy-news/asteroid-2018-cb-graze-earth-friday-watch-online/>
- Laser Bee Project, 14 May 2014. <http://www.planetary.org/explore/projects/laser-bees/>
- List of asteroid-discovering observatories. [https://en.wikipedia.org/wiki/List\\_of\\_asteroid-discovering\\_observatories](https://en.wikipedia.org/wiki/List_of_asteroid-discovering_observatories)
- Maizer A et al (2015) Space-based Infra-red discovery and characterization of minor planets with NeoWISE. In: Pelton JN, Allahdadi F (eds) *Handbook of cosmic hazards and planetary defense*. Springer, Cham, pp 583–590
- Mooney C, Dennis B. Climate change warning is dire. *Washington Post*, PA1 and A22. 8 Oct 2018
- NEOCam: finding asteroids before they find us, JPL NASA. <https://neocam.ipac.caltech.edu/>. Last accessed 8 Oct 2018
- Pappas S (2018) Electro-Blob under Africa may be 'Ground Zero' for Earth's magnetic field reversal, 1. *Space.com*, 10 Mar 2018. <https://www.space.com/39942-africa-blob-earth-magnetic-flip.html>
- Pelton JN (2015) Introduction to the handbook of cosmic hazards and planetary defense. In: Pelton JN, Allahdadi F (eds) *Handbook of cosmic hazards and planetary defense*. Springer, Cham, pp 583–590
- Pelton JN, Marshall P (2010) *MegaCrunch: ten survival strategies for 21st century challenges*. Emerald Planet, Washington, DC
- Sohn E. Gravity tractor as asteroid mover. *Science News*. <https://www.sciencenewsforstudents.org/article/gravity-tractor-asteroid-mover>. Last accessed 8 Oct 2018
- The International Astronomical Union (IAU) Minor Planet Center. <https://www.minorplanetcenter.net/iau/mpc.html>. Last Accessed October 15, 2018
- The K-T mass extinction event, exploring Earth. [https://www.classzone.com/books/earth\\_science/terc/content/investigations/esu801/esu801page01.cfm](https://www.classzone.com/books/earth_science/terc/content/investigations/esu801/esu801page01.cfm). Last accessed on 10 Oct 2018
- The Spaceguard Central Node. <http://spaceguard.rm.iasf.cnr.it/>. Last accessed 10 Oct 2018
- UN Asteroid Defense Plan, *LA Times*, 28 Oct 2013. <http://www.latimes.com/science/sciencenow/la-sci-sn-un-asteroid-defense-plan-20131028-story.html>





# Active Debris Removal for Mega-constellation Reliability

# 54

Nikita Veliev, Anton Ivanov, and Shamil Biktimirov

## Contents

Introduction .....	1044
Simulation Model for Satellite Mega-constellation Reliability X .....	1045
Concurrent Engineering Approach for SpaceX Starlink .....	1045
Reliability Simulation Model for Satellite Constellation .....	1045
Propagation .....	1046
Simulation Process .....	1048
Replenishment Scenarios .....	1049
Marketing Model for Satellite Mega-constellation .....	1050
Pricing Model .....	1051
Population Map and Market Penetration .....	1051
Agent-Based Ground Network .....	1054
Model Validation .....	1054
Commercialization of ADR and Insurance Strategy .....	1055
Conclusions .....	1060
References .....	1060

## Abstract

Provided that the hazard of space debris in orbit can pose threats to space exploration missions and, thereby, influence the redundancy of Earth observation and telecommunication constellations, this chapter addresses the case for mega-constellation reliability. The space security challenge in this case does not only relate to the regulatory and legal framework thereof but also to the business development of technical solutions for space security. Although the current level of technologies enables active debris removal (ADR), its business applicability remains to be investigated. In this study, a multiparametric mega-constellation model has been developed to take into account orbital motion, coverage, ground communication, reliability, collision risks, and service consumption in the global

N. Veliev (✉) · A. Ivanov · S. Biktimirov  
Skolkovo Institute of Science and Technology, Moscow, Russia  
e-mail: [n.veliev@skoltech.ru](mailto:n.veliev@skoltech.ru); [a.ivanov2@skoltech.ru](mailto:a.ivanov2@skoltech.ru); [shamil.biktimirov@skoltech.ru](mailto:shamil.biktimirov@skoltech.ru)

telecommunication market. The research and simulations performed on the model allowed for the analysis of possible financial metrics (revenue, cash flows, total replenishment cost) of the company who operates the ADR, as well as replacement scenarios and weak points of the mega-constellation. All combined, the chapter provides insights into the market that exists for ADR technologies, by demonstrating the ADR business applicability for mega-constellations.

---

## Introduction

Since the inception of mega-constellation projects, the space debris problem got worse. Despite the fact that the history of spaceflight has witnessed cases of collisions between operating satellites and space junk, space debris objects have not been seriously considered in the business of aeronautics. Provided that the space telecommunication market utilizing low Earth orbit (LEO) and medium Earth orbit (MEO) becomes larger, the demand for new satellite systems and constellations, respectively, grows. Hence, the density of the satellites and other objects in orbit is growing as well. Eventually, by 2030 the number of the manmade objects in LEO and MEO is expected to grow ten times bigger than it is right now (European Space Operations Centre 2019). This definitely has repercussions for the market and as it constitutes a high financial risk.

Accordingly, this chapter examines the problem of space debris and how to potentially tackle it. The solution to the problem is what has been discussed for at least a decade: active debris removal (ADR), which is based on the mechanical process of returning the space object to the Earth atmosphere. Along with a passive debris removal, which is based on the phenomenon of atmospheric drag, active debris removal is one of the main space debris mitigation methods. The approach of this chapter is based on the premise that a satellite constellation operator and a company, aiming at the development of active space debris removal, could create a mutually beneficial situation. This would allow the operator to lower the risks of collisions, increase the stability and quality of the service, and improve its financial indicators while the ADR company would position itself in the market. At the same time, ADR can be of benefit to all mankind by ensuring the sustainability of the outer space environment.

Additionally, the analysis was based on the creation of a simulation environment that could facilitate in general the analysis of business reports for the whole telecommunication market. In particular, the simulation environment could become a quite effective instrument that enables risk assessment, market benchmarking, market specification, and selection of the appropriate business strategy. Hence, the simulation of in-orbit processes and the assessment of the data links were selected as the methodology of this chapter. For this purpose, the sustainable and stable simulation environment was created with valid and verified models. This environment has included different time scales, operating scenarios, constellation types, and satellite types to estimate financial metrics of the operator. As a final stage, the study applied the simulation environment developed to the specific business study. It was produced for the ADR company working along with the first echelon of the SpaceX Starlink constellation.

The results of the simulations and the results of the analysis showed that the loss of satellite could significantly influence the quality of the service reducing the coverage rate up to 20% and lead to extremely high financial losses for the operator (up to one billion dollars for a half of the lifetime of the satellite). That said and taking into account space technology readiness level and existing and developing business strategies, the ADR could successfully enter the space market and become profitable.

## Simulation Model for Satellite Mega-constellation Reliability X

### Concurrent Engineering Approach for SpaceX Starlink

The first baseline of this study was the research made by the Skoltech Space Center, which applied concurrent engineering methods in practice. The object of the research was the SpaceX company Starlink (Kharlan et al. 2018). The work included assessment of the statements of the company (displayed in Table 1) over its work, methods, service, and implementation process. Thus, the tasks of the team included validation and reverse engineering of the technical part.

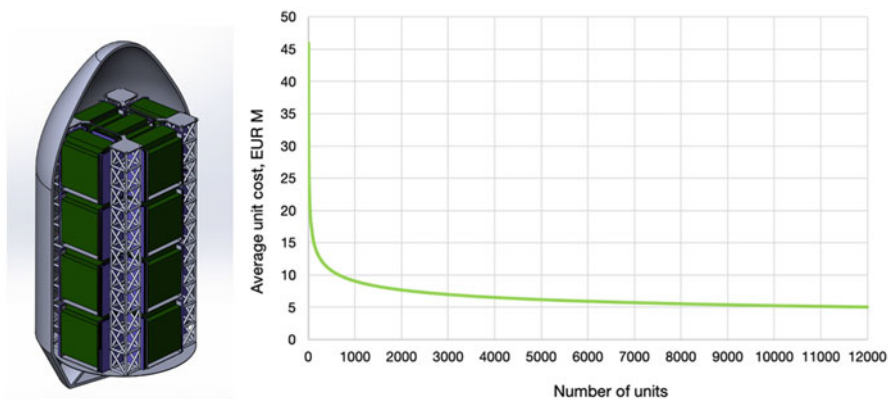
The concurrent engineering approach assesses the applicability, the main technical parameters, and the evaluation of potential financial metrics of the company, as well as possible bottlenecks of the project (Shishko 1995). Accordingly, a team of ten Space Center researchers and students conducted the breakdown of the SpaceX Starlink satellites to subsystems (Kharlan et al. 2018). The process of concurrent engineering design consisted of seven sessions and five iterations based on the use of a special software. For the purposes of Skoltech Concurrent Engineering Design Laboratory, the CDP4-IME software created by RHEA Group was selected as the best solution because of its open-source code that supports the needed functionality. The research was finalized in a month with results described in the article prepared for the IAC conference in 2018 (Kharlan et al. 2018). Some particular research outcomes are displayed in Fig. 1 exposing the mechanical part 3D model and cost distribution.

### Reliability Simulation Model for Satellite Constellation

Accordingly, the rationale for the simulation model was to understand whether the satellite is operational or not over time. Hence, the evaluation of a satellite's possible lifetime, which is generated based on the reliability distribution, becomes the most

**Table 1** SpaceX statements regarding service and project characteristics (SpaceX 2017)

Parameter/unit	Value
Mass of the satellite, kg	400
Overall cost of the project, billion US\$	<10
Connection speed, MB/s	>512
Service cost, \$	<300 per subscription



**Fig. 1** Results of the reverse engineering of the SpaceX Starlink project: mechanical 3D modeling and composition (left), average cost distribution chart (Wertz et al. 2011) (right)

crucial part of the model. The main challenge presented in the process of sampling the lifetime of the satellites is the reliability distribution as the function of time, as that becomes the statistical task. The solution can be found by compiling the data of the launch date and the failure date (if any) of all satellites available in the database of the space objects currently located in orbit. The statistical learning based on the data for satellites and space debris is listed in the SpaceTrack closed database (Caset and Saleh 2009). The overall approximation numerical formula which can be used for the calculations is (Caset and Saleh 2009)

$$R(t) = 0.000120114 * \frac{\exp(0.000265681 * t^{0.4521})}{t^{0.5479}} \quad (1)$$

where  $t$  is time in sec.

The next step of the reliability assessment was to generate the array of satellite states – the matrix describing the status of the satellite during whole lifetime was “1” for operating, “2” for interrupted, “3” for failed, “4” for being on replacement, and “0” for not working. This provided for a simple and obvious understanding of the status of the satellite during every step of the simulation.

## Propagation

This study has considered part of the upper echelon of SpaceX non-geostationary orbit (NGSO) satellite system to demonstrate economic feasibility of various ADR strategies. The SpaceX satellite system was expected to be deployed during the first deployment phase (see Table 2). The echelon comprises of 4,425 spacecraft operating in the Ku and Ka bands. According to SpaceX (SpaceX 2017), upper echelon consists of five sub-constellations corresponding to different orbit altitudes and

**Table 2** Orbital parameters of the SpaceX NGSO satellite constellation (SpaceX 2017)

Parameter	Initial deployment (1,600 satellites)	Final deployment (2,825 satellites)			
		32	8	5	6
Orbital planes	32	32	8	5	6
Satellites per plane	50	50	50	75	75
Altitude	1,150 km	1,110 km	1,130 km	1,275 km	1,325 km
Inclination	53°	53.8°	74°	81°	70°

inclinations as shown in Table 2. During this research, the first sub-constellation – corresponding to altitude of 1,150 km above the Earth and 53 degrees – was considered because of the fact that it is planned to be deployed earlier than others. This helps demonstrate operation performance of satellite communication systems. Therefore, it is worth modeling possible advantages and risks of active debris removal technologies at this step.

The satellites in NGSO are located in circular orbits and evenly distributed according to the Walker constellation design pattern (Larson and Wiley 1992). This allows placing the satellite within the constellation in a way that ensures evenly distributed Earth coverage and avoids possible collision between satellites. The main parameters of the constellation according to the Walker design pattern are the total number of spacecraft  $T$ , number of orbital planes  $P$ , and phasing parameter  $F$  (Larson and Wiley 1992). Due to the lack of information regarding the phasing parameter, it was set equal to one, which is suitable for constellation of this size.

The propagation model enables the prediction of satellite's position and velocity at a required time (Larson and Wiley 1992). Each spacecraft in constellation is equipped with propulsion system for phasing maneuvers and orbit maintenance (SpaceX 2017). Therefore, the effects of atmospheric drag and solar radiation pressure can be omitted because they mostly influence the shape of the orbit, but not the precession (Larson and Wiley 1992). Thus, the perturbation caused by Earth's oblateness is taken into account. Right Ascension of the Ascending Node (RAAN) velocity is

$$n_{\Omega} \approx -\frac{3J_2\mu_G^{1/2}R_E^2}{2R_0^{7/2}}\cos i \quad (2)$$

where  $R_0$  and  $i$  are radius and inclination of the orbit,  $R_E = 6378.245$  km is the Earth's mean equatorial radius,  $\mu_G = 3.986 \cdot 10^5$  km<sup>3</sup>/s<sup>2</sup> indicates the gravity parameter of the Earth, and  $J_2 = 1.082626 \cdot 10^{-3}$  is the first zonal harmonic coefficient.

As it was mentioned earlier, satellites in the constellation have circular orbits. Therefore, in order to describe satellite location in orbit, it is more convenient to use the argument of latitude denoted. The latter is equal to the sum of the argument of latitude and true anomaly. To describe time derivative of argument of latitude, the following expression is used (Vallado 2001):

$$\omega_D = \omega_o \left[ 1 - \frac{3}{2} J_2 \left( \frac{R_E}{R_0} \right)^2 (1 - 4 \cos^2 i) \right] \quad (3)$$

where  $\omega_D = 2\pi/T_D$ ;  $T_D$  is the period of satellite's revolution around the Earth, also called as draconic period; and  $\omega_o$  is mean motion of a satellite.

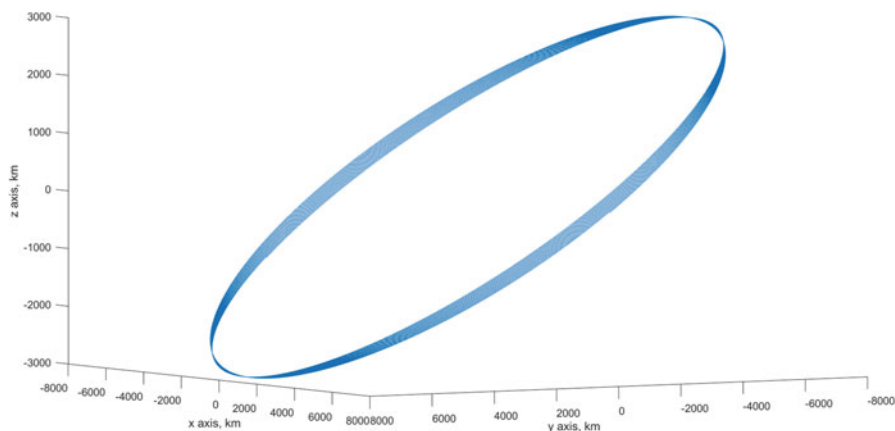
The example of 1-day propagation of the upper echelon satellite is exposed in Fig. 2.

To model the ground-track and Earth coverage of a satellite within the constellation, a projection of the satellite position was made. It was calculated in Earth-centered, Earth-fixed (ECEF), coordinate system to Earth sphere. All calculations of satellite motions made according to the previous paragraph are conducted in inertial reference frame such as Earth-centered inertial (ECI). Therefore, it should be converted to ECEF in order to calculate ground track and coverage. Transformation of coordinates is performed according to the International Earth Rotation and Reference Systems Service (IERS) 2010 conventions (Gérard and Luzum 2010) where such effects as precession and nutation of Earth rotation axis are considered.

## Simulation Process

The process of simulation starts when the majority of data is prepared for the processing. First the lifetime statuses of the constellation satellites are estimated, then the ABGN is created, and, last, the propagation matrix is ready. The initial parameters of the simulation are:

1. Simulation related parameters:
  - a. The length of the simulation period
  - b. The size of the timestep of the simulation – which definitely is supposed to be selected corresponding to the parameters of the preprocessed files



**Fig. 2** One-day propagation of the satellite taken from the upper echelon (Larson and Wiley 1992)

2. Constellation-related parameters:
  - a. Altitude
  - b. Inclination
  - c. Accuracy of the ABGN grid
3. Satellite-related parameters:
  - a. Mass
  - b. Volume
  - c. Antenna field of view
  - d. Coverage rate
4. Spare strategy type:
  - a. Two options are available: “none” for no strategy and “lod” for launch-on-demand strategy.

The process of the simulation itself consisted of a method that reads the states of the satellites and is based on information that reveals the coverage of the constellation. Moving forward, the method estimates the possible revenue and the costs for the specific timestep and finally calculates the amount of space debris in the orbit. The simulation requires much resources, including random access memory (RAM), computational power, and hard drive (HD) memory. With all the optimization, the simulation parameters were set to be constant (displayed in Table 3).

## Replenishment Scenarios

The approach of the simulation considered two types of interactions with spare issues: no strategy at all and launch-on-demand (LOD) strategy assuming that every time the satellite fails in the orbit, the other one is supposed to be launched on its place in the shortest time possible. In that case, the ADR effectiveness is supposed to be evaluated based on satellite costs and the risk of in-orbit collision assessment, which is performed using the growing collision probability formula:

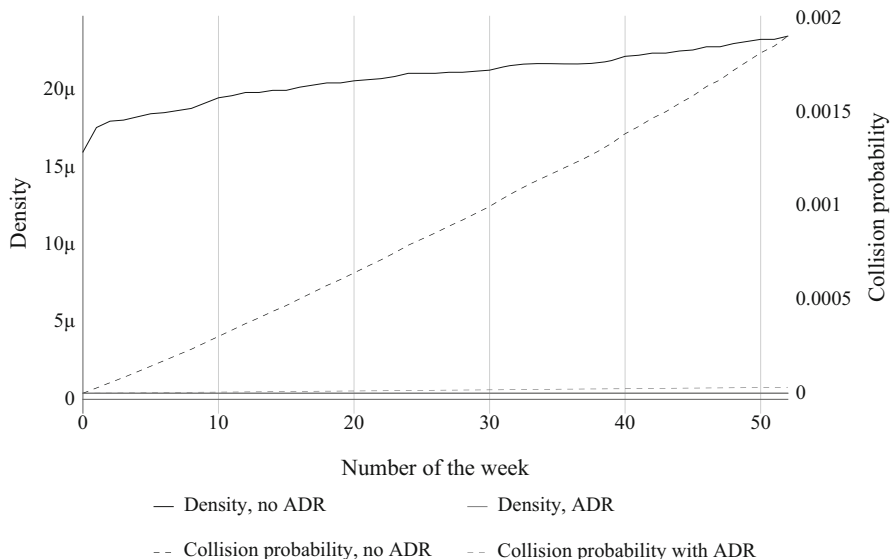
$$PC = 1 - \exp(-SPD * VR * AC * t) \quad (4)$$

where SPD is spatial density ( $n/km^3$ ), VR is relative velocity (km/s), AC is aerial collision cross section ( $km^2$ ), and t is time (sec).

In Fig. 3, the collision probability along with the growing density of the debris during the 1st year of constellation operation is displayed. As it can be clearly seen,

**Table 3** Optimal simulation parameters based on parameter-sensitivity analysis by the authors

Parameter, units	Value
CPU count, units	40
Step size, s	100
CPU frequency, GHz	3.2
Chunk size, steps	3942
RAM, Gb	200



**Fig. 3** Space debris density distribution and collision probability distribution based on simulation results of the authors

the ADR is supposed to line up the risk management and lower the probability of the chain reaction.

## Marketing Model for Satellite Mega-constellation

As long as the satellite constellation model was created and it became clear how each satellite in the constellation moves and what was the coverage of each satellite, it became available to assess how each satellite influences the connectivity and, consequently, the company operator's financial metrics. For that purpose, it was necessary to assess the market and allocate marketing data to the coordinates on the Earth surface.

Obviously, as an understanding of the possible business applications of the ADR is based on the financial metrics of the operators, the marketing analysis and model are taking the most important part in the research. It facilitates the calculation of possible revenue for the constellation through the implementation of economics and marketing.

The underlying reasoning of detailed market study was to understand the number of subscribers in every point of the Earth globe and according to the pricing estimations to calculate the potential positive and negative cash flows as a benchmark. The created marketing model consists of two major blocks:

- Pricing model
- Population model and market penetration



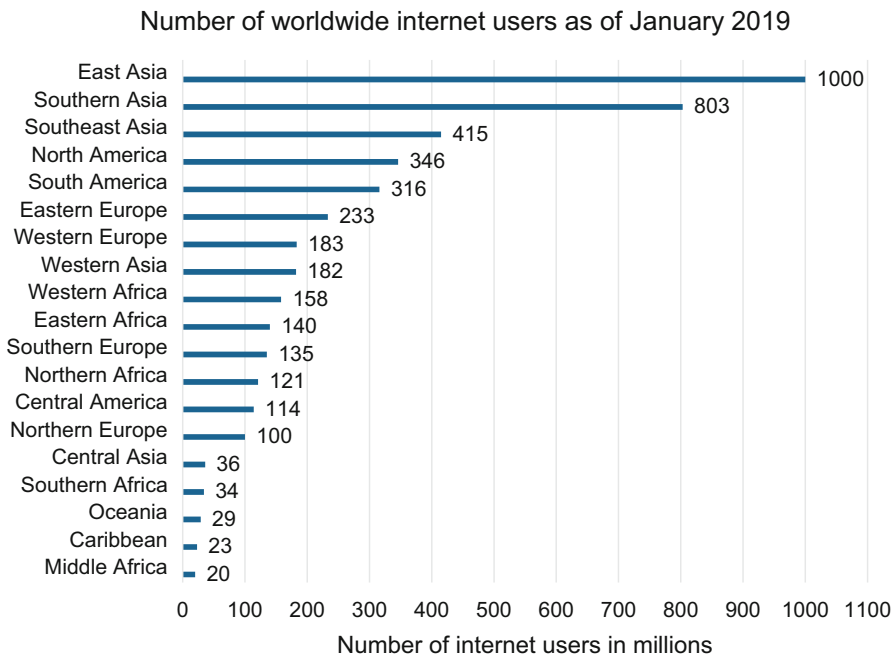
## Pricing Model

The study considered two different types of pricing currently being used by the telecommunication companies worldwide: all-flat and traffic-based tariffs (Deloitte 2019). For the flat plans, the price of the service was calculated as the average price of the flat tariff in the particular country. Figures 4 and 5 show the statistics used for the calculations of the traffic-based subscriber contract.

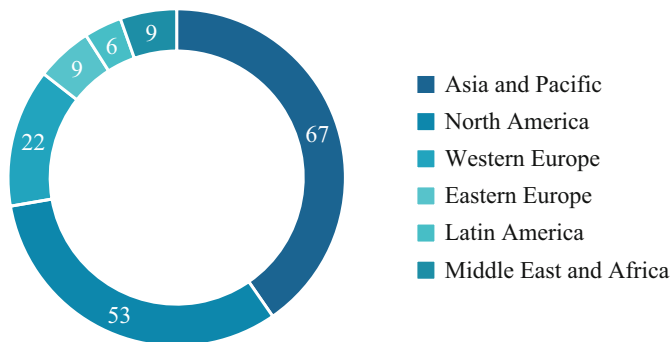
Both calculations were made and verified using the open-source data for telecommunication companies' statistics in Russia, Statista Inc. database. The average errors for both methods are shown in Table 4.

## Population Map and Market Penetration

The population data is based on the information prepared by the NASA Socioeconomic Data and Applications Center (SEDAC) (Doxsey-Whitfield et al. 2015) based on the gridded population of the world (GPW). The fourth version of the data is the distribution of the human population across the Earth. The statistical data is generated based on the Earth observations and provides globally consistent data for any type of the researches and studies.



**Fig. 4** Internet user number distribution by region (Statista Inc. database 2019b)



**Fig. 5** Internet traffic consumption per month by the region (Statista Inc. database 2019a)

**Table 4** Verification error for different pricing models, based on the simulation assessments of the authors

Method	Error rate, %
Flat	28
Consumption-based	13

The Earth observation data was transferred to the population data values; then the data passed the process of normalization using the official statistic of the countries. This work uses data for 2015 with a resolution of 1 degree. However, increasing the accuracy significantly decreases the calculation speed and affects the overall simulation time, according to Formula 5 (representing the needed number of calculation steps in order to facilitate the whole grid for a single timestep):

$$N_{steps} = \frac{180deg * 360deg}{A} \quad (5)$$

where  $N_{steps}$  is the number of steps,  $A$  is accuracy (step size,  $deg^2$ ), and  $180*360$  is altitude-longitude degree grid.

The population is not the only thing that is necessary for the calculations though. The other important elements are market penetration and target audience. Both parameters are limited to the number of users interested in the service and able to pay for it. The generic coefficient determining the part of the population that supposed to use the service of the exact provider can be estimated by the formula:

$$K = MS * I * IP \quad (6)$$

where  $MS$  is the market share,  $I$  is income availability, and  $IP$  is Internet penetration.

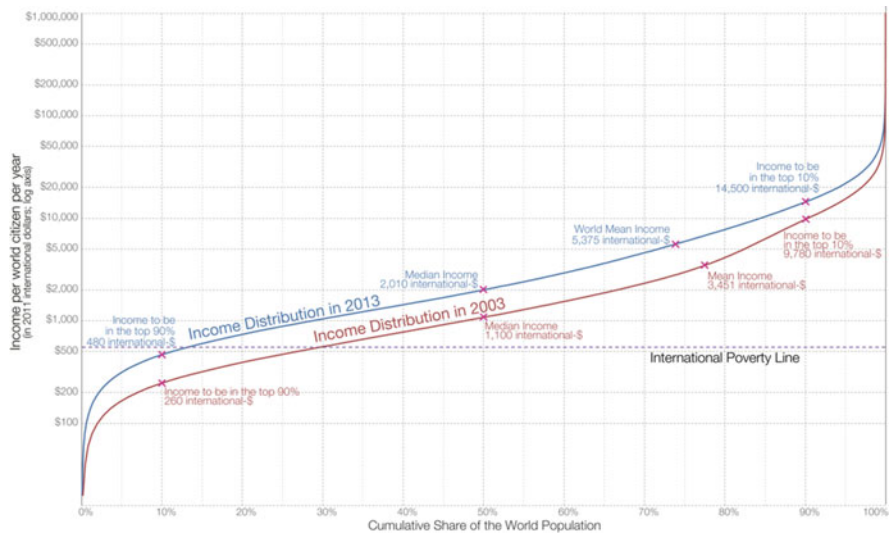
Theoretical three-parameter model describes three sides of the approach of estimation of the amount of the target audience: economic, marketing, and technical.

The market share of the company is determined dynamically as a function of time, describing the entry of the company to the market with boundary conditions. This is described in the Federal Communications Commission (FCC) request of SpaceX technical information in 2017, as well as in official forecasts of the SpaceX Starlink stating 40 million subscribers and 30 billion US dollar revenue by 2025 (Harris 2019). As a market acquisition model, the Gompertz curve (Zlatić and Štefančić 2011) has been selected, because the growth speed of the curve is pretty similar to the market share speed. The approximation was used to describe the mobile phone penetration to the population (Islam et al. 2002). The exact formula is presented in Eq. 7:

$$MS = 0.2158 * e^{-3.0716 * e^{-0.00000354 * t}} \tag{7}$$

where  $t$  is time in sec.

Income availability is the parameter describing price availability of the product on the market. This parameter is being calculated based on the price of the product and the distribution function of the income per capita in each country. According to the fact that the Internet connection payments on average are holding 10% of all spends per month (Visser 2019), selecting the tariff price gives an understanding of the number of people that are able to pay. For most countries, the shape of the curve is described with different data. However, for those countries with no data available for a “rich-poor” curve, the average worldwide curve was used. This curve is displayed in Fig. 6 as an example (OurWorldInData Inc. database 2014).



**Fig. 6** The world population income distribution in 2003 and 2013 (OurWorldInData Inc. database 2014)

## Agent-Based Ground Network

Considering the output of the economical modeling process, the agent-based ground network (ABGN) has been created. The term ABGN as well as the grid itself was created during the research specifically for the simulation to simplify the process of markets of the Earth-based consumers. The ABGN is the operational set of agents, or in this case subscribers of the Internet service, integrated to the peer-to-peer-linked network distributed by the Earth globe and having a set of parameters, enabling the assessment of the entire system. In the case, when the subscriber is a single user or a household, the agent network could be represented as the grid with number of the subscribers in surrounding area as the nod value.

Each agent can be represented as an object of the “subscriber” class with a set of attributes. This is based on a self-made Python class of objects containing a set of parameters with relative information regarding the selected type of the subscriber. The attributes are:

1. Position. The positional argument, describing the position of the subscriber (or a set of subscribers) on the Earth globe. The distribution could be random, functional – set up with a function of time, evenly weighted – normally distributed nodes of the grid, setting up a single subscriber or number of subscribers in the surrounding area, or single-located, the array of coordinate of the subscribers.
2. Money capacity. The parameter of money capacity is being calculated based on the amount of the target audience in the nod and the price of the service. This parameter is the permanent base for the calculations of the money flows of the operational company and dynamic coverage methods.
3. Traffic demand. The parameter is calculated based on the amount of target audience in the nod and the traffic demand in the location per capita. This parameter hardly influences the link budget and dynamic coverage methods.

The agent-based ground network is able to represent not only the large number of users but the single user as well. In other words, this system works with both the business to consumer (B2C) and business to business (B2B) strategy of operation problems. That, in particular, allows to solve the static and dynamic tasks (or a combination of such). This advantage allows the model to be applicable to other scenarios for various companies. The system works on a plug-and-go basis meaning that setting up the type of the ABGN does not require changing code in the core of the simulation.

## Model Validation

As soon as the environment is ready, the verification takes place in order to determine the applicability of the model to real scenarios. The validation has been delivered as a two-step process: the first one was the validation of the model itself,

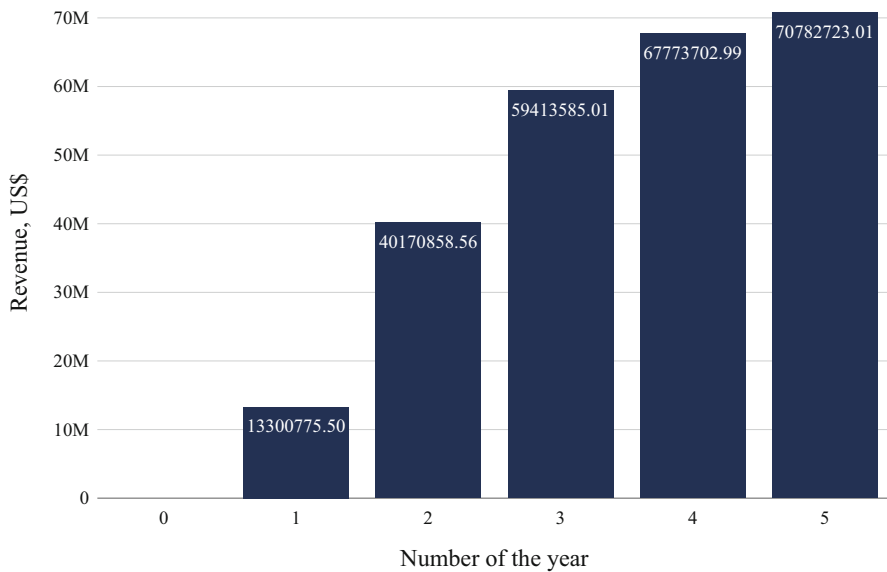
performed with running the simulation for the constellation that already exists; the second was the case validation, determining whether the model is applicable to the particular case study.

In the first part, the simulation process was run with the characteristics of and information about the Iridium Inc. constellation (from annual report to Stockholders in 2009) that has been firstly launched in 1997 and consists of 75 active satellites with a coverage of 100% of the Earth globe. The idea was to compare the results of the simulation with company open data (including revenue). The outputs are displayed in Fig. 7, with the error made up to 7%.

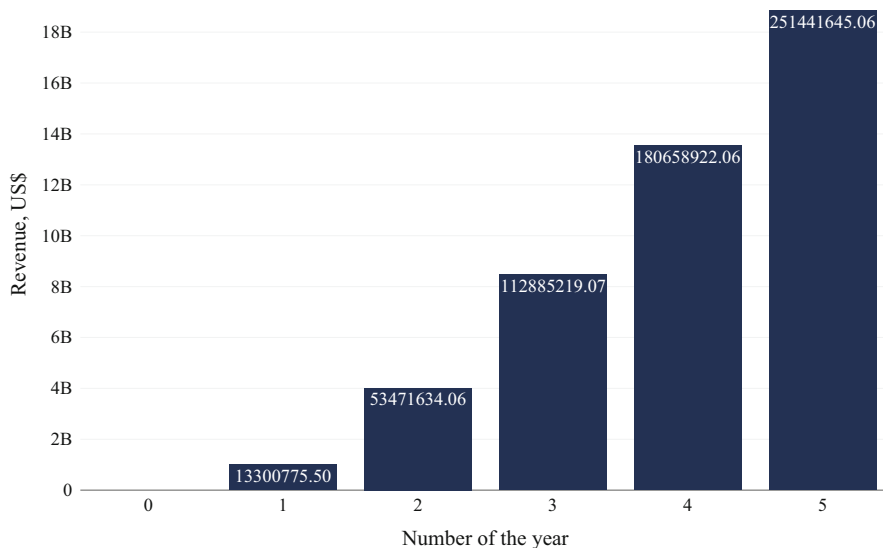
The case validation was based on the open data of the SpaceX company official statements claiming the amount of revenue by 2025 (claiming 30 billion US\$ of revenue by the time) (Mosher 2019). The error appeared to be 122%, as the results display in Fig. 8. The big error is corresponding with lack of data.

## Commercialization of ADR and Insurance Strategy

According to the baseline of the simulation, the propagation and coverage footprint were calculated. Based on the coverage and reliability model, the overall constellation coverage was calculated. Along with created ABGN model, the possible market coverage of the operator was calculated for the selected satellite constellation formation. The data for each timestep gave an opportunity to understand main



**Fig. 7** Annual yearly revenues for the Iridium Inc. simulated, where year 1 is the 1st year after main launch in 2003 based on simulation results of the authors



**Fig. 8** Annual yearly revenues for the SpaceX simulated, where year 1 is the 1st year after main launch in 2020 based on simulation results of the authors

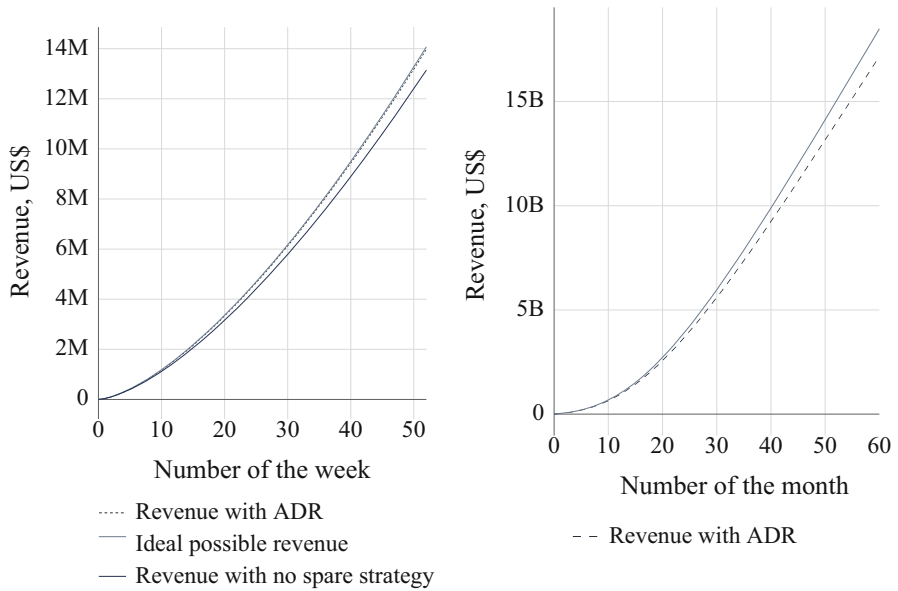
financial metrics of the operator (such as positive cash flow from the servicing, income, and operational expenses).

This, consequently, enabled the research group to run some basic assessment scenarios of the telecommunication segment. The environment and the models have been verified using the existing cases of constellations and open information of the company at hand.

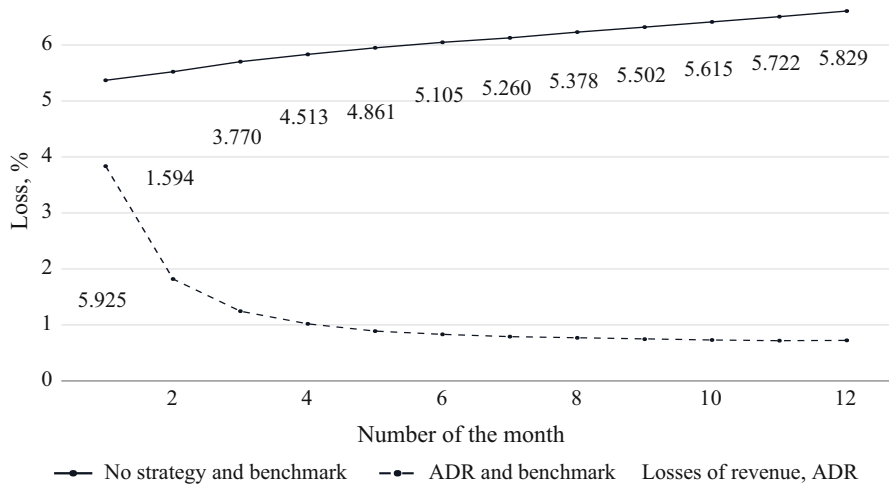
Afterward, the environment was used several times to assess the satellite service to be provided and supported by the SpaceX Starlink company for the simulation periods equaled to 1 month, 1 year, and 3 years. The output data is represented as a time evolution of several important parameters: revenue flow, costs, space debris density in orbit, and coverage. The results are exposed in Figs. 9, 10, and 11.

Following the assessments made in the beginning of the work, losing the satellite led to several huge impacts on the constellation operational indicators. It can be seen in Fig. 9 that operating with no replenishment strategy could be followed by revenue decrease (around 1.5 mln USD for the 1st year and nearly 1 bln USD for the first 5 years). In Fig. 10, the same data showed in percentage which is up to 6% revenue loss for the 1st year. Figure 11 also shows that the malfunction satellite can also lead to a coverage loss leading to the quality issues.

The assessment showed that active debris removal is critically important for the company-operator as it allows to increase revenues and decrease the risks of collisions. The main result of the outcome analysis is the fact that ADR is not only practically necessary to tackle the challenges of the mega-constellations, but it can also be commercialized.

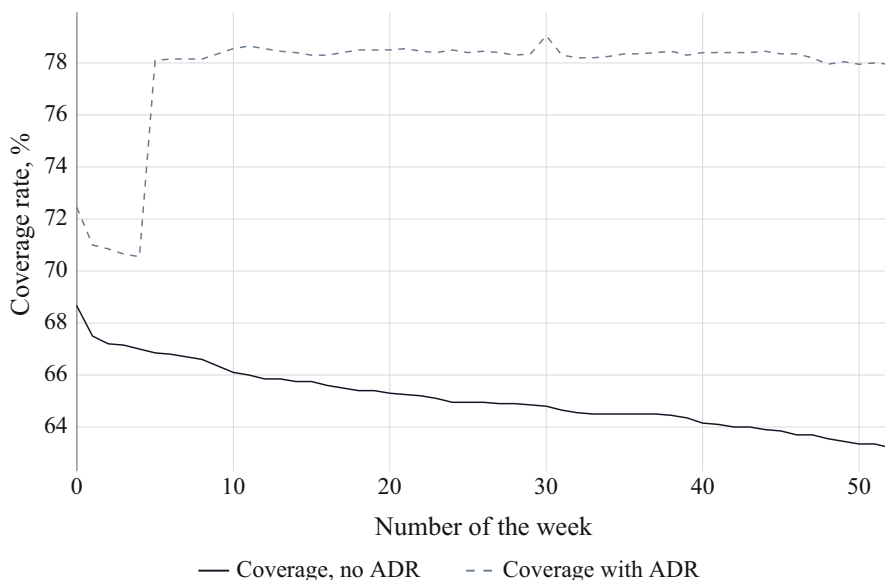


**Fig. 9** Revenue time evolution for the case study: simulated for 1 year (left) and for 5 years (right) based on simulation results of the authors



**Fig. 10** Revenue losses for the consequent periods based on simulation results of the authors

Based on the research outcomes, a marketing analysis was followed to create a sustainable business strategy for the ADR company. For that purpose, the company was evaluated from a business perspective. The analysis showed the specifics of the business and possible strategy options. Three major business plans



**Fig. 11** Time evolution of the coverage based on simulation results of the authors

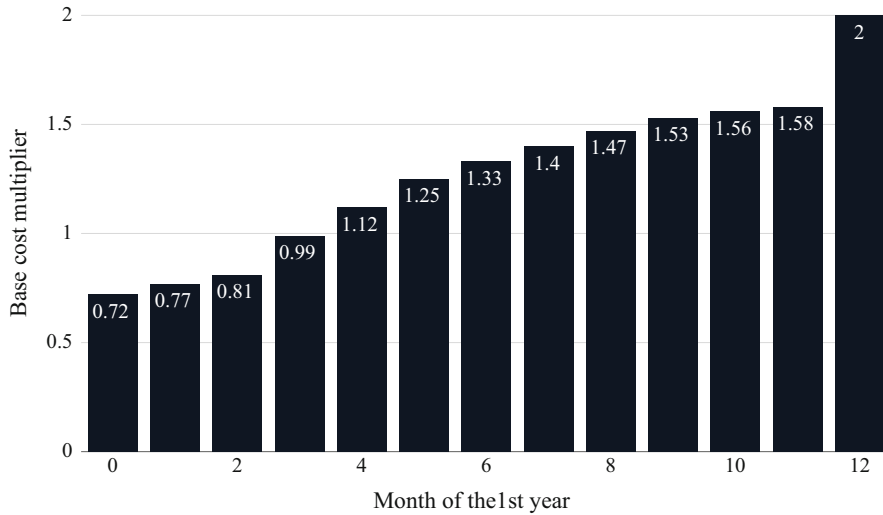
were assessed: the “flat insurance,” the “dynamic flat insurance,” and the “pay-as-you-go tariffs.” For each of the strategy, a separate simulation turn was run in order to understand the applicability of the strategy, its profitability, and positives and negatives of its use.

The flat insurance strategy is based on the business plans of the insurance and reinsurance companies providing the full insurance. This includes the complete ADR services, for a fixed reward. After simulating, this plan, however, appeared to be noncompetitive since the reward calculated is quite high and appears to be not advantageous for the operator.

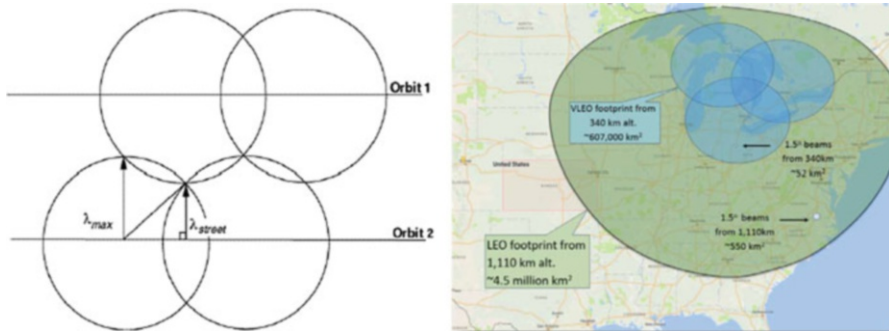
The pay-as-you-go tariff, on the contrary, means to implement the system of rewarding the ADR company every time the satellite replacement takes place. However, in that case, things can get worse for the company itself. Since the satellite failure is highly connected with the reliability of the satellite, it seems that the company’s financial behavior can turn to be unpredictable. This can subsequently lead to investment overlaps and breaks – the incomes of the company are going to be strictly connected to the satellite loss, which is not equally distributed over time – the cash flow becomes “jumping.”

The compromise lies in merging both of two options and adjusting the details of the strategy. The dynamic flat insurance implements the dynamic rewarding methods and selective ADR use. The rewarding technology is connected with the distribution of the satellite reliability over time, taking into account any kind of collision risks. In Fig. 12, the rewarding scheme is presented. The rewarding scheme based on the business plan enabling dynamic price change; in that case, the price depends on the overall reliability of the constellation. It means that the more time the constellation





**Fig. 12** Reward strategy: base cost multiplier distribution over time based on simulation results of the authors



**Fig. 13** Footprints of SpaceX lower echelon (SpaceX 20,187) (right) and “street size” description (left)

lives, the less its reliability, the more money the customer supposed to pay to cover the ADR service.

Additionally, the simulation showed that the loss of one individual satellite has approximately no influence on the service quality, while the failure of two coherent satellites leads to 1.5 times as big revenue losses. This actually is explained by the fact that the satellite coverage footprints overlap as it can be clearly seen in Fig. 13 (Kharlan et al. 2018) – the blue circles are displaying some of the first echelon satellite footprints. The picture shows that the loss of one satellite leaves relatively small piece of Earth surface, which can lead to predictable and short connectivity losses. At the same time, losing several consequent

satellites significantly increases the uncovered surface bringing continuous and unbalanced connectivity failures.

---

## Conclusions

The objective of this chapter was to analyze a business case connected with an active debris removal (ADR) process. It aimed to understand its applicability and prove the market existence for ADR. In order to pursue this investigation, the analysis was based on the creation of a simulation environment for mega-constellations, the Starlink SpaceX first echelon constellation. The results of the study give insights into the success of an ADR company, being interconnected with the role of operators of these large constellations.

[Can you summarize here a bit more about the results? I think they are very important to highlight in relation to the mega-constellation challenge].

Despite the importance of the results, the limitations of the method are evident due to the study performed for the specific large case of mega-constellations. In order to address these limitations, future research could look into the following proposed directions:

1. Perform a study for different constellation with different orbital parameters.
2. Perform a study for different altitudes (MEO and GSO).
3. Perform a study for other markets, such as Global Navigation Satellite System (GNSS), Earth observation (EO), or defense applications.
4. Apply different optimization methods.
5. Assess the replenishment times and the constellation sizing factors.

---

## References

- Castet JF, Saleh JH (2009) Satellite and satellite subsystems reliability: statistical data analysis and modeling. *Reliab Eng Syst Safe* 94(11):1718–1728
- Deloitte Center for Technology, Media and Telecommunications (2019) Telecommunications industry outlook. <https://www2.deloitte.com/content/dam/Deloitte/us/Documents/technology-media-telecommunications/us-telecom-outlook-2019.pdf>
- Doxsey-Whitfield E, MacManus K, Adamo SB et al (2015) Taking advantage of the improved availability of census data: a first look at the gridded population of the world, version 4. *Pap Appl Geogr* 1(3):226–234
- European Space Operations Center (2019) ESA's annual space environment report, 5, pp 1–77
- Gérard P, Luzum B (eds) (2010) IERS conventions. Technical note no. 36. Bureau International des Poids et Mesures, Frankfurt am Main
- Harris M (2019) The space-wide web. *New Sci* 242(3228):44–47
- Iridium Communications Inc (2009) Annual report to Stockholders, Accessed 28 Feb 2019. [https://investor.iridium.com/download/IRDM\\_10-KWrap2009.pdf](https://investor.iridium.com/download/IRDM_10-KWrap2009.pdf)
- Islam T, Fiebig DG, Meade N (2002) Modelling multinational telecommunications demand with limited data. *Int J Forecast* 18(4):605–624

- Kharlan A, Ivanov A, Veliev N et al (2018) University-based facility for evaluation and assessment of space projects Alexander Kharlan. In: 69th international astronomical congress, Bremen, pp 1–5
- Larson WJ, Wiley J (eds) (1992) Space mission analysis and design, 3rd edn. Microcosm Press, Torrance
- Mosher D (2019) SpaceX may be a \$120 billion company if its Starlink global internet service takes off, Morgan Stanley Research predicts, Business Insider. <https://www.businessinsider.com/spacex-future-multibillion-dollar-valuation-starlink-internet-morgan-stanley-2019-9>. Accessed 28 Sept 2019
- OurWorldInData Inc (2014) Global income distribution. <https://ourworldindata.org/global-economic-inequality>. Accessed 4 Mar 2019
- Shishko R (1995) NASA systems engineering handbook. National Aeronautics and Space Administration, Washington, DC
- Singh N, Browne LM, Butler R (2013) Parallel astronomical data processing with Python: recipes for multicore machines. *Astron Comput* 2(8):1–10
- SpaceX (2017) Spacex V-band non-geostationary satellite system attachment a technical information to supplement schedule S. International Bureau Application Filing and Reporting System, FCC. Available at: [https://licensing.fcc.gov/myibfs/download.do?attachment\\_key=1190019267199/global-consumer-internet-traffic-by-region/](https://licensing.fcc.gov/myibfs/download.do?attachment_key=1190019267199/global-consumer-internet-traffic-by-region/). Accessed 15 Mar 2019
- Statista Inc (2019a) Global consumer internet traffic by region. <https://www.statista.com/statistics/267199/global-consumer-internet-traffic-by-region/>. Accessed 15 Mar 2019
- Statista Inc (2019b) Number of internet users worldwide. <https://www.statista.com/statistics/273018/number-of-internet-users-worldwide/>. Accessed 15 Mar 2019
- Vallado DA (2001) Fundamentals of astrodynamics and applications, 2nd edn. Microcosm Press, El Segundo
- Visser R (2019) The effect of the internet on the margins of trade. *Inf Econ Policy* 46(3):41–54
- Wertz JR, Everett DF, Puschell JJ (2011) Space mission engineering: the new SMAD. Microcosm Press, Hawthorne
- Zlatić V, Štefančić H (2011) Model of Wikipedia growth based on information exchange via reciprocal arcs. *Europhys Lett* 93(5):58005



# Space Security and Sustainable Space Operations: A Commercial Satellite Operator Perspective

# 55

Jean François Bureau

## Contents

Introduction .....	1064
Space Operations in GEO .....	1065
Space Operations in LEO, MEO, and Transit Orbits .....	1069
Protection of Satellites Services from and at Earth .....	1072
Conclusion .....	1075
References .....	1078

## Abstract

The increasing need of commercial Satcom services (for governments, economy, social, and cultural purposes) augments the call for a coherent “space security” discussion which will lead to the development of rules and guidelines for sustainable space operations. Two main items of utmost importance to commercial space operators are elaborated in this chapter: the management of space operations in increasingly “crowded orbits” and the protection satellite services should receive, both in space and on Earth. During the last two decades at least, guidelines, best practices, agreed principles, and “soft law,” have been the pragmatic answer to move forward. However, the exponential increase of space-based services will call for a “governance framework” which should strengthen the principles of the Outer Space Treaty and ensure that the Treaty will remain effective in the coming decades.

Views expressed in this article are the author’s one only, and cannot be Eutelsat ones.

J. F. Bureau (✉)

Institutional and International Affairs, Eutelsat Group VP, Paris, France

e-mail: [jbureau@eutelsat.com](mailto:jbureau@eutelsat.com)

## Introduction

Since the United Nations Group of Governmental Experts (GGE), established in 2011 (GA Res A/RES/65/68, January 5th 2011) and concluded its report on “Transparency and Confidence Building Measures in Outer Space activities” (A/68/189 of July 29, 2013) (TCBM) in 2013, the discrepancy between space security requirements and space risks and challenges have significantly increased.

The TCBM proposal identified by the UN GGE has been largely ignored in terms of implementation, and the failure of the EU Code of Conduct proposal as well as the deadlock on the discussion of the long-term sustainability (LTS) guidelines created a sense of “no hope” on the diplomatic discussions. At the same time, the large and rapid changes that have taken place in the last 5 years in the field of space-based services and applications, as well as the disruptive innovations that supported a lot of new projects especially in low orbits (including the so-called mega-constellations), have increased the urgency for a more space security organized environment, considering the overall sustainability of space activities.

The 50th anniversary of the Outer Space Treaty in 2017 was not an occasion for many events. This low attention probably reflected a more substantial question about the extent to which the Treaty and its framework of international conventions (first of all the International Liability for damage caused by space objects Convention of 1972 and the Registration of objects launched in outer space Convention of 1975) would still shape the coming developments of human activities in and from space in the future. In addition, how the Treaty and related Conventions provisions would be resilient enough and inclusive enough to shape and regulate all coming developments which are under preparation.

The nonappropriation of outer space, along with the freedom of exploration, the liability for damage caused by space objects, the prevention of harmful interference with space activities, and the obligation to notify the international community and to register space activities are all legally acknowledged principles. (But, during the last period of time, different projects seem to assume that the nonappropriation of Outer Space could allow for the privatization of the mining of asteroids.) Yet, they are challenged, either because they are bypassed, or because they are discreetly ignored, or even openly violated.

Last but not least, and even if the prohibition of placement of nuclear weapons or other weapons of mass destruction in outer space seems to be still in force, the number of warnings that a new round of technologies could prepare for a militarized space is obvious. To quote the famous assessment from the US National Security Space Strategy of 2011, “space, a domain that no nation owns but on which all rely, is becoming increasingly congested, contested and competitive.” (US Office of the Director of National Intelligence: “National Security Space Strategy,” January 3, 2011.)

All these trends are feeding the sense that space could become an out-of-rule domain, a kind of jungle of the twenty-first century which will undermine many coming projects, or even destabilize the most established space-based services.

Because a part of the new revolution links together space-based systems and commercial services, in an increasing number of applications, be they civilian, military, or dual, commercial operators (be they “old” or “new” space) perceive the forthcoming environment as challenging. The concerns include not only an increasing lack of regulation, but also essential space dependency for many more activities on earth. According to the US Commerce Secretary Wilbur Ross, “today, the global space economy is roughly 400 billion dollars, about 80% of which is commercial activity” but “Morgan Stanley projects the global space industry could reach 1.1 trillion dollars by 2040.” (Remarks by US Commerce Secretary Wilbur L. Ross at the US Chamber of Commerce Space Summit, December 6th 2018. Office of Public Affairs, US Department of Commerce.) As an observer remarked, “so the department (of commerce) is trying to deregulate the industry, making it easier for entrepreneurs to jump in, and to lure capital from venture capital firms, hedge funds, sovereign wealth funds and even mainstream pension funds.” (Tett 2018; see as well, Donohue 2018.)

As space becomes a truly essential service base for a large spectrum of human activities on Earth, security of all the stakeholders (States, private, and international organizations), resilience of the regulations which allow and organize those services, sustainability of the infrastructure deployed in space, and finally, predictability of the upcoming rules based on a truly world-wide consensus constitute the ingredients of a safe and secure space for the future. No need to say that to overcome this challenge, which is multilateral by nature, requires a lot of effort and willingness from all stakeholders.

From a satellite operator perspective, three sets of key issues can be listed, which could, altogether, jeopardize the future of its activities, in terms of development, sustainability, and affordability. In this time of “crowded orbits,” (refer to Moltz 2014) (1) it is tempting to identify these challenges at the geostationary orbit; (2) at the juncture between the geostationary orbit on one side, and the medium-earth orbit and low-earth orbit on the other; and (3) finally on earth as presented in the following sections.

---

## Space Operations in GEO

As already suggested, the most crowded and congested orbit is the geostationary orbit where 548 of the 1886 existing satellites are positioned, 1186 being in LEO orbit and 112 in MEO. (Data provided by the Union of Concerned Scientists “Satellite database” in its update of August 10th 2018, Accessed 12 Dec 2018.) It is interesting to notice that in 2012, 1050 satellites were in operation, among which 432 were in geostationary orbit, 73 in medium-earth orbit, and 503 in low-earth orbit. (The figures are provided by J. C. Moltz, in “Crowded orbits,” op.cit pp. 20–23.) These figures deliver quite a strong message: the GEO orbit is now growing very slowly in terms of new satellite populations, as opposed to LEO that is witnessing a dramatic increase of resident space objects.

GEO orbit is crowded and congested to such large extent that the management rules for the fleets raise more constraints. Yet the core of the International Telecommunications Union (ITU) regulation of the space-based services for telecommunications is still mainly based today upon the noninterference principle as it was at the beginning of the 1970s, when the management of the orbital positions was far less constrained. The change is such that, at that time, the management of the orbital positions was also complemented by another implicit rule – first arrived, first served – which cannot any longer be implemented. Of course, the principle of non-interference is of much importance as it allows for proper technical functioning of the satellites at close orbital positions, through coordination agreements among operators, but appears too limited to address all potential situations.

Among them, the dynamic management of fleets, the appearance of a graveyard orbit, and the emergence of “clinging satellites” are quite troubling and may illustrate the extent to which existing regulations are not able to face the coming challenges. Basically, the need for enduring transparency about what is happening at the GEO orbit and “who” does what may have to be on the top of the to-do list the international community could set up. It is assumed that one key obstacle of such transparency has been, in the past, the importance of military services which were provided by military satellites at this orbit, especially for nuclear testing detection, early warning of missiles launching, or detection of preparations for a military offensive. Such missions are for sure still needed even if the geopolitical and strategic environment is nowadays profoundly different from the Cold War one, and the satellites associated with them may legitimately receive a different treatment.

However, managing transparency at the activities which take place at the GEO orbit, from the satellites which are registered by the UN Register now ratified by 68 nations and some intergovernmental organizations (like Eumetsat, Eutelsat, ESA, or Intersputnik) at the end of 2018, would also be the beginning for more security in orbit, keeping in mind that, according to the UNOOSA, 91% of all satellites, probes, landers, crewed spacecraft, and space station flight elements launched into Earth orbit or beyond have been registered with the Secretary-General. (UN Office for Outer Space Affairs (UNOOSA) website, Register of Objects Launched into Outer Space, Accessed 12 Dec 2018.) From that standpoint, it is important to notice that the Registration Convention is still attracting new signatures, like the Luxembourg one, a nation which has recently decided to join the Registration Convention. However, registration should probably be based on a wider basis than a very administrative process. Like ships and planes have received an identification once the management of their movements was obviously needing a way to track them to prevent fatal collisions, providing an ID to the registered satellites may be the next needed step to ensure that the Registration Convention will still be a significant tool for space governance.

As we shall see, absence of even minimal rules related to transparency at the GEO orbit is providing an avenue to behaviors which are obviously dangerous, and which could become common because of the impunity the players which are behaving so do feel. The fact that impunity prevails over responsibility and accountability is obviously not a good situation.

Because of the saturation at the GEO orbit, operators need to develop a very dynamic “fleet management” which includes increasingly frequent satellites movements along the orbit. (As an example Eutelsat which owns close to 40 satellites has had to manage an average of 5–6 moves each year since 2011 (however of very different magnitude), and there is no doubt that the frequency of these moves has increased along these years.) For that reason – ensuring that close movements by different satellites will not create harmful interferences or even collision risk among them – the satellite telecommunications operators have established a shared and common database of technicalities associated with each satellite they operate, which can facilitate safe movements and close locations, and by itself could illustrate the kind of best practice and transparency which could be extended to all registered satellites. (The database is managed by the “Space data association” (SDA). SDA “is to seek and facilitate improvements in the safety and integrity of satellite operations through wider and improved coordination among satellite operators and to facilitate improved management of the shared resources of the space environment and the radiofrequency spectrum” (SDA website consulted December 13, 2018). SDA is now looking at enlarging its database to other orbits than GEO.) From a regulatory perspective, and in order to comply with ITU rules related to the orbit management, satellite operators have noted that a frequency assignment can be brought into use only if a satellite is maintained at the orbital position for a continuous 90-day period so fighting against “paper satellites,” and that from another standpoint, a frequency assignment cannot be suspended for a period exceeding 3 years. All these rules which ITU has developed in order to better manage the orbit and allow access to it to all newcomers are also aimed at limiting the cases where “force majeure” is claimed. It is fair to say that these rules, because they are more and more constraining, are also creating business opportunities among satellite operators, which will need each other more often to ensure the continuity of service to their customers, when the scarcity of orbital positions and frequency assignments do not allow for mismanagement of these “rights.”

It must be added that national legislations can also contribute to this transparency. In the case of France, satellites movements are notified 1 month in advance to the French space authorities, as an obligation deriving from the French Space Operations Act of 2008. However, there is no binding international rule creating the same obligation at the moment, even if recommendations to notify such movements have been adopted by UN member states. In a nutshell, guidelines based upon transparent behaviors and explicit rules for the orbit management to be followed by all parties to the Register Convention will be ever more needed, and in the interest of all stakeholders, will be.

National Space Laws (like the 2008 French one) also include provisions aimed at ensuring the protection of the space environment during the satellites’ life cycle, which means proper control of the satellite during its in-orbit life (station-keeping, relocations) and deorbiting at the end of its operational cycle in ways which will minimize the risks for health and the environment. Those rules are directly derived from some guidelines and best-practices recommendations established under the UNOOSA via its COPUOS technical works, as part of the space debris management



issue. However, for this last part, the guideline is based upon the principle that the satellite must be able to reach a position (the “graveyard orbit”) located at 300 km above the GEO orbit, and that, once at that final position, the satellite has been totally passivated and will no longer be a threat of any kind (energy, mechanics, radio-frequency, health). For sure, this deorbiting rule is providing a rule aligned with the fact that those satellites, beyond any kind of reach from earth at 36,000 km, cannot be of any use. However, it should be recognized that we are only at the starting point of this “graveyard policy” and that many satellites launched since the beginning of the last decade has still to reach the graveyard. Hence, there is some doubt that this rule will be sustainable in the long term, as the number of out-of-cycle satellites will quickly increase in the next 5/10 years because satellites launched in the 2000s will have to be replaced, in order for operators to keep the orbital positions they have been authorized to use and from which they provide services.

Finally, the principle of “noninterference” does not prevent “passive hostile” attitudes like the situation by which an unidentified satellite is coming so close to your satellite that it enters the “box” where this last one is supposed to be maintained in order to serve properly and in due compliance with the noninterference principle, and this unidentified satellite clings to your satellite for a period of time which can be a matter of months, and not only of hours or days. Despite the obvious danger such a behavior entails, this passive hostile attitude does not allow for complain, in absence of interference. However, a satellite which is stationed for a long time close to another one which has the full rights to stay at its orbital position, in its “box,” is potentially dangerous, even from an orbit management perspective, and finally, could be considered as a serious threat, and as such in breach of the basic rules of peaceful uses of outer space. Every behavior of such nature should be accountable, and transparency rules should request for compulsory statements by which the nation responsible would have to explain the reasons of such close presence at an orbital position (the “box”) which is not supposed to be the harbor of a passive, but potentially hostile, clinging satellite. It is obvious that along the last years this story of clinging satellites has expanded to a point that, after US officials raised the issue during the Space 50 Conference, the French ministry of Armed Forces also made it publicly when she revealed that a French-Italian satellite (ATHENA-FIDUS) had been spied by a Russian satellite (Luch (Olymp-K)) without any kind of governmental comment or official justification. It is well known that other Russian satellites have behaved in the same way along the last years with different commercial satellites owned by several different satellite operators. That the existing rules, or more precisely their weakness, can allow such movements and “passive aggression” demonstrate the magnitude of the gap which is now created between what could be considered as a responsible management of the GEO orbit and what is taking place. The next step in such an escalation of dangerous behavior will obviously be that a commercial satellite is facing a situation where its integrity is at stake and takes initiatives for movements which could, at the end, turn into a collision between the two objects. Even if the article IX of the Outer Space Treaty calls for a conduct of all space activities “so as to avoid harmful contamination” and asks countries to notify other countries before engaging in any activity that might cause “harmful

interference” with activities of others, there is no regulation, procedure, and even concrete sanctions that could limit such attitudes and even prevent them. If there is a will to restore a safe and secure use of the space domain, the most efficient way to prevent such an escalation is to make such attitudes public (as the US and French officials did recently), make them transparent, and strengthen the rules which must prevent them. The shame of the present situation is that such behavior is even not clearly in breach of the rules, despite the very significant danger posing for the stability and safety of space-based activities and services. An increase of global space situational awareness (SSA) capabilities and a “naming and shaming policy” should put an end to the impunity that some stakeholders make use of.

---

## Space Operations in LEO, MEO, and Transit Orbits

It has already been noted that one of the most disruptive changes taking place at the moment is the quick and significant development of projects planning to use the low-earth orbit (LEO), and to a lesser extent the medium-earth orbit (MEO). The magnitude of change is such that some consultants foresee 6500 smallsats to be launched in LEO orbit before 2027. (NSR press release about its report “Small satellite markets,” 5th edition, Accessed 28 Nov 2018.) Other figures have even been mentioned, like 11,943 satellites, authorized by the FCC, which are planned by M. E. Musk constellation “Starlink,” (Wall Street Journal (online), Accessed 18 Dec 2018) or the 3500 satellites One Web is intending to deploy. Should all the projects already made public by developers and startups be implemented, a total of 18,000 satellites could reach the LEO orbit before the end of the next decade.

Obviously, such an order of magnitude is creating a lot of unknown challenges, but the significance of this change can be measured against the fact that the world aeronautics industry looks for more than 36,000 planes in service in the world in 2032 (against 17,740 in 2013) which will transport 6.3 billion travelers. In other words, and assuming that most of the current projects will be implemented, where we were seeing roughly 1 satellite against 10 planes in the mid of the 2010s, the ratio could become 1 satellite against 2 planes in the mid of the 2030s. In addition, it must be noted that, in many cases, these new low-orbit constellations will aim at providing connectivity in planes, like many key geostationary already decided (e.g., Eutelsat VHTS) will do. This new connection between telecommunications satellite deployments and air fleets development could be of structural consequence for both domains in the next future.

These disruptive figures may give a sense of one new and key issue which will have to be faced: the organization of the management of the different orbits, and the notion that the different orbits will have to be understood in their dynamic interaction.

At the moment, the main regulatory guideline, issued by the ITU in 2007 along with the “noninterference principle,” states that the signal coming from the GEO satellites shall not be interfered by signal from satellites at lower orbits, the GEO signal being far less powerful when it reaches the earth than the other signal,

especially those emitted from LEO satellites. These rules have been set up for the Ku and Ka bands which are providing the most significant services (Ku for television by satellites, Ka for internet and connectivity by satellites).

The wording of the ITU stands as follows (Radio Regulation No 22.2, as decided by WRC-07):

*22.2§ 2Non-geostationary-satellite systems shall not cause unacceptable interference to and, unless otherwise specified in these Regulations, shall not claim protection from geostationary-satellite networks in the fixed-satellite service and the broadcasting-satellite service operating in accordance with these Regulations. No. 5.43A does not apply in this case.*

These rules may have to be strengthened. However, new parts of the spectrum, like Q- and V-bands, will be extensively used by satellites systems, notably to connect the earth gateways and the satellites in the coming decade. Most of the “very high throughput satellites” (VHTS), like those designed by Thales Alenia Space and/or Boeing, will make use of these Q- and V-bands.

Those issues are listed on the WRC19 agenda (Agenda Item 1.6 of WRC19). In order to prepare for that discussion, the WRC15 (2015) asked to conduct and complete in time for WRC-19:

*1 studies of technical and operational issues and regulatory provisions for the operation of non-GSO FSS satellite systems in the frequency bands 37.5–42.5 GHz (space-to-Earth) and 47.2–48.9 GHz (limited to feeder links only), 48.9–50.2 GHz and 50.4–51.4 GHz (all Earth-to-space), while ensuring protection of GSO satellite networks in the FSS, MSS and BSS, without limiting or unduly constraining the future development of GSO networks across those bands, and without modifying the provisions of Article 21; (. . .).*

In addition to the large and (maybe) numerous constellations in LEO related to telecommunications services, the coming Internet of Things (IoT) constellations and the maturation of the observation market which will drive the deployment of dedicated constellations, like Planet6Labs which plans for 140 low orbit satellites, must be considered. These two kinds of applications will, for sure, include an increasing number of artificial intelligence (AI) assets, which will be on-board small (like shoe boxes) and unexpansive satellites. (The New York Times International was referring to satellites of 7000 \$ a piece, Accessed 12 Dec 2018.)

With these new developments, space-based services are reaching a kind of industrial age which they ignored until now, despite the more than 42,000 TV channels currently broadcasted globally by satellite. AI and IoT will for sure drive a standardization process, in terms of production, and a development of satellite-based services unknown until now. In addition, new assets, like balloons, high altitude pseudo satellites (HAPS), and drones, will become part of the connectivity networks deployed in space. As well, suborbital flights will have to be considered in terms of legal and regulatory terms, and it will have to be decided whether they should be regulated by the air-space rules or by the space

management principles, both systems needing to be (at least partially) aligned to be manageable.

The industrial age of the space-based applications will entail new services like in-orbit services. These services intend to extend the life cycle of the satellites by refueling them (when their propulsion is mainly chemical) and/or repairing some of their major components like solar antennas. A few companies are currently planning for such in-orbit services. However, this next step is already raising a lot of questions: if space services ability to extend the life cycle of the satellite can be affordable, do we need to plan for 15 years of life cycle for the telecommunications satellite, as it was done until recently or should we think about less duration for the satellites (8–10 years for example) with a better ability to adapt the services to the consumers expectation, when planning for the market in 2030 is so difficult?

Such in-orbit services would entail an increasing level of space movements and traffic which would need specific regulations but are still to come. It has been said that soon the first “mission extension vehicle” (or “space tug”) will be launched to extend the life duration of Intelsat 901. Assuming that this interest in life-extension of the satellites could be shared by other satellite operators, what will be the legal status of these objects? Should they be registered like satellites? What is the consequence if such an object fails to provide the service it was assumed to? What is the status of such an object if left in space? Is it a debris, and if so, could the Liability Convention apply? All these questions need to be addressed quite urgently as there is no common rule already agreed. Furthermore, because of the growing number of LEO projects, which will entail hundreds of launches, the overall effect of this change will be an increasing number of debris, even in absence of military activities aimed at testing anti-satellite weapons.

Space surveillance, including space surveillance and tracking, will therefore receive a growing attention from all space users. SSA and Space Traffic Management (STM) are, for the time being, sovereign missions, developed by governments or groups of governments (the EU plans to develop its own capacities). The condition under which these data could be shared with commercial operators, will have to be decided. At the commercial level, the SDA has outsourced a capacity of that kind, adjusted against commercial needs (of course very different from the military needs, and much more limited than them) and allow for access to data to the contributing operators. In the future, the growing importance of such SSA/STM data is so great that the US government has decided that the US Department of Commerce would become the interface with the commercial satellite operators in terms of SSA data sharing. This recent change could also open the door to established commercial SSA and STM services which would complement the governmental ones. If that is the case, they need to decide how these SSA/STM data from different sources will be shared, and along which rules these will be of much importance.

Two questions will be of key importance in order to ensure a sustainable space operations environment:

- How will all stakeholders of the space-based infrastructures, among them the private satellite operators, have access to the space surveillance awareness data? It

can easily be assumed that not all data will be accessible, but according to the “need-to-know” principle, there is room to decide which of them are of interest for the commercial operators.

- To which extent the dedicated tools, implemented and managed by governments or groups of governments, will be phased with the pace of the commercial services development? If it is recognized that the SSA data could be shared if and when a denial of service could be intended, an obvious threat to some assets could be experienced, or more broadly, in order to better understand the new developments which could put satellite operators at risks, then SSA policies would strengthen private policies aimed at ensuring continuity of service and agreed service levels.

For sure, satellite operators will consider SSA and STM as key strategic issues which should be inclusively designed. The way to proceed and the roadmaps to be defined will become major issues of the relationship these commercial operators will have with governments. However, if we take into account GEO management challenges, LEO/MEO developments, and multiplication of space objects (like space tugs), there is no doubt that the entire Space Situational Awareness and/or Space Surveillance and Tracking purposes and methodologies have to be redesigned in accordance with the disruptive changes which are going to take place in the way all space stakeholders will make use of this common good.

---

## **Protection of Satellites Services from and at Earth**

Since the core business of telecommunications by satellites has moved from direct-to-home (DTH) TV broadcasting to internet and broadband services, the value of the different components has faced a major shift: when the DTH broadcasting was mostly an investment in the space segment in the 1990s, which represented more than 90% of the total (space + terrestrial) investment, the space segment is about 60% of the total investment when it comes to broadband services by high throughput satellites (HTS) which are based upon a multispots coverage. In other words, around 40% of the investment is nowadays related to the terrestrial segment of the space-based system. This terrestrial segment is mainly distributed between gateways which connect the final user equipment (antenna + modem) to the internet, through the satellite. The network of gateways, installed in different places (nations) throughout the coverage of the satellite, constitutes a distributed hub managing the traffic and the spectrum allocation to and from different satellite spots.

This architecture which is becoming the standard of connectivity provision in the GEO high and very high throughput satellites (VHTS) will become even more essential in the LEO constellations in order to ensure continuity of service when the constellation “flies” over a location.

Hence, protecting the terrestrial gateways and networks from interferences, be they technical (deliberate or not), legal, or even political, is crucial. This matter is mostly regulated by nations, according to their conceptions of “internet freedom,”

the resilience of the technical solutions selected by the internet service providers (ISP), the security regulations which apply to these networks, and more widely, to the broadband policies decided by governments.

The freedom of information has been defined in 1948 by the UN Charter on Human Rights as: “Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions with-out interference and to seek, receive and impart information and ideas through any media and *regardless of frontiers*.” (article 19).

The UN Covenant on Civil and Political Rights (1966) developed its consequences as follows:

Article 19.1. Everyone shall have the right to hold opinions without interference.

2. Everyone shall have the right to freedom of expression; this right shall include freedom to seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.

3. The exercise of the rights provided for in paragraph 2 of this article carries with it special duties and responsibilities. It may therefore be subject to certain restrictions, but these shall only be such as are provided by law and are necessary: (a) For respect of the rights or reputations of others; (b) For the protection of national security or of public order (ordre public), or of public health or morals.

The fact that both of these documents state that freedom of information must not be limited by frontiers receives a special meaning in the case of internet by satellite, which is by nature, the most efficient tool to disseminate information “regardless of frontiers.” However, the worldwide trend seems to look for more constraining rules, in many cases for security reasons. How to ensure free provision of space-based services and freedom of information at the internet age, on one hand, and security requirements, on the other hand, at the same time needs to be considered not only at the level of the governments, in charge of setting national rules, but also at the international level, which is appropriate to set rules aimed at implementing the principles as stated by the UN Covenant, which is binding for ratifying states. Previous attempts to move forward in this direction have failed in the past, when TV dissemination was the main satellite service. However, the new development of space-based services will call for more determined actions to update the implementation of these lasting principles which have to be protected in this new situation, as well.

From another standpoint, the new era of space-based services will look at the convergence between telecommunications and navigation services (like GPS and Galileo). If connectivity has to support mobility, both kinds of services will be needed at the same time, and the satellite will be, again, an indispensable tool because of its territorial coverage, when terrestrial telecommunications network (i.e., fiber, 4G) basically address urban and concentrated populations. With the 5G coming, the end user will ask for a seamless connectivity, every time and everywhere. This expectation, which will ensure continuity of service, will request hybrid and complementary networks, terrestrial and space together providing a resilient

service based on a large interoperability of the networks, able to match any kind of unexpected situation as the satellite will also provide the back up to the terrestrial network in case of need, or in case of urgency. Such architecture will allow for satellite to serve remote, distant areas, and mobility needs when terrestrial networks will first of all provide services in highly dense and urban areas. Furthermore, the resilience of the overall supply will extend the spectrum of applications, especially to the very demanding services related to defense and security, as we already noticed.

Along this change, the clear-cut separation between defense/security needs and commercial needs will continue to blur. There is already a lot of security/defense needs which are fulfilled by commercial objects and operators; military planners are now including the commercial assets in their assessment of the resources which could be mobilized in case of need by governments (because of the flexibility provided by large commercial fleets), and commercial operators consider the governmental needs as a key driver for their future development (i.e., EU Govsatcom in Europe which should include services provided by commercial operators; DISA reform in the United States by which the Air Force Space Command will “oversee management of nearly all military and commercial SATCOM for the DoD” (US Air Force Space Command press release, Accessed 12 Dec 2018). Furthermore, disruptive technologies like software-driven satellites will allow the best provision of the power and of the spectrum based on end user needs. (The “Quantum” satellite, to be launched in 2019, and built by Airbus in UK, will be the first 100% software-driven satellite.)

If governments and operators together develop collaborative policies and solutions to fulfill the security needs, more robust rules will have to ensure that hostile actions against commercial satellites will be treated in the same way as hostile actions against sovereign satellites. However, the requisite for such approach is the ability to designate the origin of the hostile action, in other words the ability to attribute. Here, the challenge is probably of the same nature as it is when it comes to cyber-attacks. In both cases, satellite jamming and cyber-attacks, the actors bet on the impunity they can expect from the difficulty to identify their behavior and to attribute the unlawful practice. Hence, and even if new satellite technologies allow for anti-jamming equipment and geo-localization mechanisms on-board the satellite, which become quite conventional on commercial satellites, it seems that satellite manufacturers need to invest in research and development to ensure that those which are tempted to make use of cyber-attacks or jamming of the signal will be deterred from such behavior because of the increasing risk of being identified. Again, being able to “name and shame” the origin of the infringement and the identity of the rule breaker, like a whistleblower, is a must. To the extent that such infringement is facing a sanction!

Government’s responsibility in case of jamming of the satellite signal falls under the ITU rule: however, despite recent progress from the ITU Pleny Potentiary of 2014 (resolution to set up a database of the geo-localized jamming), the fight against deliberate jamming (for political reasons, to prevent the reception of a signal in a territory) must be strengthened. Western nations are currently the only ones which may be ready to recall the principles, and more important, to ensure that they are still implemented by the community of nations which are UN members.

Space security must be understood in a comprehensive way: it is not only about protection of the space segment. A space-based infrastructure is a system combining a space asset and a network of terrestrial gateways/infrastructure which are as important as the space segment in order to provide the service. This terrestrial component of the space-based system has an increasing strategic value as it is the service provider component to reach the end user: we can observe an increasing pressure from governments to receive a right to have access to or even to be able to control the flows of data coming from (or going to) the satellite. There are good reasons for that (e.g., fight against terrorism), but there are also very serious threats resulting from that trend (reduction or even suppression of freedom of information). The international community has established strong grounds which have supported the development of the space applications (like TV and internet services provision), which is the freedom to access to information “without borders consideration”; (art 19 UDHR; art 19 of ICCPR; EU HR Chart): these principles are obviously challenged in an increasing number of situations.

Space operations and space services are at the core of the discussion about cybersecurity in space. They all need very dynamic and robust cryptology methods in order to ensure that the very quickly increasing number of services based upon space infrastructure will be resilient to adverse behaviors. New technological developments like laser transmission of data (EDRS in EU; NASA next generation relay satellite/post TDRSS) is giving the space-based solution some kind of advantage to ensure the security of the data transmissions: the space community (governments, industry and operators) should identify the contribution the space-based solutions can bring to a more secure cyber environment, and set up the rules which will strengthen this key advantage at the moment when satellite services are even more needed.

---

## Conclusion

Along the last decade, it has been expected that this need for a more regulated environment for space-based activities could be fulfilled by guidelines, best practices, and agreed principles. This set of rules will be even more needed in the coming future than it already is. As the governmental, economic, and social value of the space-based applications multiply, such rules will only protect the proper management of the humanity “common good” which is the space domain.

If there is no deployment of offensive weapons systems (like ASW) in space, this “soft law” recommendation should concentrate on two main issues, which unite most of the described situations: service (and access to) denial; attribution of action (transparency/responsibility/liability).

However, it should be recognized that, with its code of conduct proposal, the EU tried to make steps forward towards a more sustainable space environment. The failure of such proposal to reach the consensus shows how important it is to strengthen the efforts. It seems that far from being the “common good” subject to peaceful activities, as described by the Outer Space Treaty of 1967, it moves towards



a kind of jungle where survival and security of the services, whatever their nature, will not be granted.

Looking at the plans to develop new activities related to space exploration and the prospect of “celestial commercialization,” a commentator was stressing that “the time has come to clarify international space law and allow commercial ventures to go ahead subject to sensible safeguards.” Noting that “a full-scale revision of the Outer Space Treaty might be desirable but is not necessary,” this comment was suggesting that “a governance framework agreed by all spacefaring countries would do the job.” (See Financial Times, “The world should update its laws on outer space,” Accessed 28 Dec 2018.) This cautious approach was taking stock of the very difficult challenges a revision of the Treaty would entail at a moment of hardened competition among the space nations, and despite the benefit all humanity could find from an updated treaty which could decide for the regulations of the coming and extended space activities. However, far worse, deciding for a revision of the Treaty could open a Pandora box which could, finally, undermine the principles which the Treaty has recognized and which are still very meaningful for the future. Should a Treaty revision be decided, it should aim at strengthening those principles, and set regulations which would help to manage the coming challenges, not destroy the “space order” which is still based upon the Treaty.

Obviously, and in absence of a “consolidated” Treaty, the governance framework which is required is more than urgent, and not only because of the asteroids commercialization. Space is at the juncture of sovereign and commercial activities, national and international projects, closely related to the emerging data and digital needs and technologies, close to extend significantly the number of industries and services which will rely on it on a constant basis. More than an infrastructure, space-based activities are becoming the most ubiquitous domain which most not to say all future human development plans will require. Absence of governance, allowing all these plans and services to find their path will become a challenge from which, in absence of significant progress, the mere future of this attractive and even exciting new area could collapse without delivering its promise.

International organizations, governments, and private actors must now bend their efforts to establish this governance framework which is so much needed.

In that respect, commercial operators should build upon their own experience of space-based services to further contribute to shaping this framework. Among the different items they could raise, some seem more urgent.

A first priority could be to develop the *transparency* of movements in space. As an example, adding a satellite identification to the registration obligation could help monitoring movements at the different orbits, facilitate their notifications during the 15 years of the life cycle of many satellites, and discriminate satellites from space tugs and high altitudes balloons or drones, for example. History shows that such transparency (based on an ID) was the condition for a safe and secure use of the airspace by planes, and seas by ships. It can be doubtful that the huge increase of

space objects in the near future will allow for an enduring regime of quasi-secrecy about the movements in space, even more if collisions between space objects were to remain nonliable.

The second aspect could be to develop a *responsibility* scheme where international norms, best practices, and/or national space laws, financial incentives finally could combine to promote a sustainable use of space. The launching industry has demonstrated a significant capability to reduce the risks of failures in the launching business because of the attention the operators paid to the insurance cost of the launchings they ordered. The need for an insurance could be extended to more space activities, and could act as an incentive to develop designs which could reduce the number of debris, extend the life time of space assets, or reduce the collision risks (especially at low orbits).

The third aspect should tackle the absolute need to ensure the *continuity* of service which end users are expecting from the space rules and actors. The guarantee of service continuity is the condition for an area of large recourse to space-based services, especially if these services deal with connectivity and mobility. It should encompass the prevention of deliberate interferences, the technical developments which will ensure the robustness of the signals against cyber-attacks, the ability to identify and designate the parties which are threatening the continuity of service. A lot of investment (technical and financial) is paid to achieve this service continuity objective, but it needs to be backed by rules which will penalize the actors undermining it.

A final dimension could set up the appropriate forum where all issues related to space sustainability and governance could be discussed between international organizations (CD, COPUOS, ITU. . .), governments, and private actors (the list of which is extending quite quickly). At the moment, all concerned entities develop their “own” framework for discussion, but these different discussions are not coordinated along with a *common agenda* which could have been agreed by all stakeholders. The need for an agreed “space agenda” which would answer the questions – what are the issues at stake? what are the key priorities to address? to which extent proposals and identified solutions can be implemented by the actors, need “soft law” solutions (best practices, standards. . .), or need an urgent “hard law” (conventions, revised OST) – all these issues need to be addressed in a forum which could report to the UN, as the ultimate responsible for a safe and secure space.

Security and sustainability of space-related activities is facing a very serious challenge. Commercial space operators have an insight on technological developments (which they very much drive when ordering the space-based and ground-related infrastructure), affordability of coming services (especially in terms of connectivity and data management), added value of space-based services (by comparison to terrestrial solutions), and regulations which could support the space based economy. All these issues cannot be solved by one government, or even one international organization. They are multifaceted, evolving, and pressing at the same time.

## References

- Donohue TJ (2018) CEO of the US chamber of commerce. Space, the new economic frontier. Space News, December 17, 2018
- Moltz JC (2014) Crowded orbits. Conflict and cooperation in space. Columbia University Press, New York
- Tett G (2018) Space: the final frontier for finance. Financial Times Magazine, December 19, 2018



# Space Debris Mitigation Systems: Policy Perspectives

# 56

Annamaria Nassisi, Gaia Guiso, Maria Messina, and Cristina Valente

## Contents

Introduction .....	1080
Current Situation of Space Debris and Risk Posed to Long-Term Sustainability .....	1081
Drawing Analogies Between Outer Space and Maritime for the Regulation of Space Debris .....	1082
Need for New Rules Ensuring Sustainable Development for the Evolution of Satellites ...	1083
Ongoing Search for Space Authority .....	1084
ITU Role in Leading Regulation on Space Debris .....	1085
ITU Role in Guaranteeing Space Security Against the Debris Threat .....	1086
Discussion: Fairway Charges in Space, a Starting Point for Space Debris Regulation? ....	1087
Conclusions .....	1088
References .....	1088

---

A. Nassisi (✉)  
Strategic Marketing, Thales Alenia Space, Rome, Italy  
e-mail: [annamaria.nassisi@thalesaleniaspace.com](mailto:annamaria.nassisi@thalesaleniaspace.com)

G. Guiso (✉)  
Women in Aerospace-Europe (WIA-E), Milan, Italy  
e-mail: [gaiaguiso@gmail.com](mailto:gaiaguiso@gmail.com)

M. Messina (✉)  
Education Unit, Italian Space Agency (ASI), Rome, Italy  
e-mail: [maria.messina@est.asi.it](mailto:maria.messina@est.asi.it)

C. Valente (✉)  
Marketing and Sales, Telespazio, Rome, Italy  
e-mail: [cristina.valente@telespazio.com](mailto:cristina.valente@telespazio.com)

---

**Abstract**

The preservation of the space environment against space debris threats requires the development of a legal and regulatory framework. The sustainability and ongoing security of the space environment requires an agreement at international level. The study argues that in order to develop a set of specific rules for the governance and regulation of space debris it might be helpful to draw on similar contexts. First, maritime law on salvage on the high seas, developed by the International Maritime Organization (IMO), can facilitate the approach to abandoned spacecraft. Second, the role of international organizations such as the International Telecommunication Union (ITU) can serve as a point of reference in the development of binding space debris mitigation rules. The development and implementation of such rules will contribute to the successful sustainability of outer space activities.

---

**Introduction**

The chapter provides an analysis of the legal and policy issues concerning future operational debris mitigation systems. This is an essential step in preparation of specific rules, agreed at national and international level, for a legal and regulatory framework.

The analysis performed focuses the attention on these main three topics:

1. Space debris problem and need for regulation
2. Maritime law as a reference to address the rules for abandoned spacecraft/space debris
3. ITU as a reference organization that can adopt binding rules

What we need is a binding international legal instrument. Yet, as it might take too long before we have the next treaty, addressing soft law and rules of the road could be relevant. Maritime law can offer some frame of reference to solve this issue. Specifically, the international law of salvage in high seas, as outlined in the International Convention on Salvage, IMO 1989, may help to establish a similar regime, in space, for abandoned spacecraft.

In this regard, the pivotal role of the International Telecommunication Union (ITU) in setting a regulation for the Active Debris Removal missions (ADR), in the years to come, should not be underplayed. Since this agency is in charge of promoting and coordinating the definition of technical standards, as well as of assigning satellite orbits, it might be able to establish itself as the referral organization for the issuing of finally binding space debris mitigation rules. As in the case of frequency regulation, also in the case of debris mitigation and removal, it is crucial to have an institution capable of supporting the multiple stakeholders and security constraints. So much of the future of space activities will depend on how these

rules will succeed in limiting the growing amount of floating debris in space. Are the “Space debris” a threat for Space Exploration? This causes legal uncertainty.

The tendency to overcome limits confirms an unavoidable desire of knowledge, inherent in all human beings. Despite the new technology innovations, the ambitious plans relating to exploration and commercial exploitation of extraterritorial resources implies the need of a legal certainty at national and international level. Protecting outer-space from damages caused by negligence or breach of duty should foster new legislative efforts and finally a new instrument of hard law. The sovereignty aspect continues to guide the international community toward flexibility and escape clauses. If we contextualize Durkheim’s thought, the French sociologist who lived in the mid-nineteenth and twentieth centuries, we would say that managing debris as a social phenomenon involves measurement of its detrimental effects, and subjugating individual interests to collective’s one.

In accordance with the principles contained in the “Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies” (Outer Space Treaty 1967), governmental organizations aim to pursue “the benefit and the interests of all countries, irrespective of their degree of economic or scientific development.” This provision is essential for a comparative analysis between Space Law and the principles governing the Law of the Sea, especially on the sustainability and protection of natural resources.

The lack of ratification of the “Agreement Governing the Activities of States on the Moon and Other Celestial Bodies” (Moon Agreement 1979) demonstrated the difficulty to further develop the legal framework regulating activities on the Moon or other celestial bodies. Following the new geopolitical order of the 1970s, the negotiation of the Moon Agreement occurred at the same period with United Nations Convention on the Law of the Sea (1982), both echoing the intention of States to define responsibility in a newly international cooperation framework. Although United Nations Convention on the Law of the Sea (UNCLOS) and Moon Agreement are similar in terms of legal nature, the same cannot be said for the ratification process. Although the Moon Agreement has only been ratified by 13 states, it took the UNCLOS 10 years of negotiations to be ratified by 164. The Law of the Sea therefore represents an example for the progressive development of international space law.

---

## **Current Situation of Space Debris and Risk Posed to Long-Term Sustainability**

The debris population could be generated from accidental case or voluntary case. The well-known antisatellite test (ASAT) of China is an example of voluntary case where a defunct weather satellite, called Fengyun-1C, was destroyed by a missile that imparted an estimated 350 joules per gram of its mass. Another well-known

collision that we can classify as accidental case, is the 2009 collision between the Iridium33 and Kosmos2251 satellites. Both cases have produced an increment of debris population, a risk for operational satellites and a threat of sustainability as highlighted in the report of the International Interdisciplinary Congress on Space Debris: “Guidelines for the Long-term Sustainability of Outer Space Activities of the Committee on the Peaceful Uses of Outer Space (2019)(UN A/74/20).”

A lot of commercial initiatives consider solutions for space debris removal. As such, ensuring that sustainability of outer space can be realized through the promotion of progressive development of international space law. Promoting awareness of this issue should be sought through a plurality of legal and scientific efforts with a motivated incentive to open data.

## **Drawing Analogies Between Outer Space and Maritime for the Regulation of Space Debris**

The roadmap for the common spaces – the Earth and the seas – have always been a good arena for all policy makers, scientists, and economic stakeholders to discuss. Both outer space and the seas have posed significant challenges at international level. Although in both cases, the idea to set up a supranational legal framework was suspicious of any effort to control and limit freedom. As it will be indicated below, particular attention was paid to environmental management from the point of view of safety policies and protection of the marine environment: hence, the importance of drawing analogies between outer space and maritime for the regulation of space debris.

The adoption of the 1989 International Convention on Salvage and the “no cure no pay” rule (art. 12. 2 “no payment is due under this Convention if the salvage operations have had no useful result”) marked a step forward in the management of maritime environment (IMO 1989).

The International Maritime Organization (IMO) Convention calls upon States Parties:

- To carry out the salvage operation with due care (article 8)
- To take measure to protect coastline or related interest from pollution or threat of pollution following upon a maritime casualty (article 9)
- To give a reward to encouraging salvage operation (article 12)

Any analysis seeking to guarantee such protection in outer-space led to non-legally binding results. That is why the Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space (COPUOS) an example of many voluntary political engagements that have become well-established practice. The guidelines describe space debris as “*all man-made objects, including fragments and element thereof, in Earth orbit or re-entering the atmosphere, that are non-functional,*” and emphasize that rapid growth increases the probability of collision. It is stated that “*the prompt implementation of appropriate debris mitigation measures [is meant] towards preserving the space environment for future generations.*” The

use of words such as “*minimize*,” “*avoid*,” and “*limit*” contained in Space Debris Mitigation Guidelines underpin that the guarantor of their application is the recipient itself.

Even up to today, the only binding policy provisions related to the return of objects launched into outer space are contained in the Agreement on the Rescue of Astronauts, the Return of Astronauts, and the Return (The Rescue Agreement) of objects launched into outer space of 1968, but with the sole aim of recognizing duties of each contracting party and launching authority.

Nonetheless, article 5, paragraph 4 of the Rescue Agreement takes into consideration the issues of environmental protection in outer space. It is based on the provision that it is extremely important to react and eliminate any space object or its component that may be considered as potentially harmful. This interpretation could be a bit of a stretch: the agreement is mainly guided to promote international cooperation and provide all possible assistance to astronauts. Lastly, in accordance with article 6, the launching authority should pay the costs incurred to recover and return space object but, unlike the Convention on the International Maritime Organization – adopted 1948 and entered in force in 1958 – there is no reference to a possible reward. Thus, although it suggests to act and protect outer space environment, it’s not clear to what extent though. The International Convention on Salvage, IMO 1989, is crucial therefore in reference to the liability and compensation mechanism, helping states to face the challenges that remain unresolved.

## **Need for New Rules Ensuring Sustainable Development for the Evolution of Satellites**

In a world that is becoming increasingly sustainable, a new set of rules should acknowledge such a paradigm shift in outer space as well. While there have been some attempts to create a widespread endorsement of evaluation methods for the footprint of substances used in the space industry, in this regard, the Intergovernmental Panel on Climate Change (IPCC) and the European Commission’s Joint Research Centre’s Life Cycle Assessment (LCA) can be cited. Currently the legislation producing the most impact on the production chain of substances susceptible of harming the planet and the space environment, include the Montreal Protocol on Substances that Deplete the Ozone Layer (1987), the European Commission’s Restriction of Hazardous Substances (RoHS) directive (2003), and the Registration, Evaluation, Authorization, and Restriction of Chemicals (REACH) regulation (2006) – all placing restrictions on particular substances used in space programs ([ESA Safety](#)). Also in maritime law, similar agreements have been reached to protect the maritime environment: for instance, the Protocol on Barcelona Convention concerning Cooperation in Preventing Pollution from Ships and, in Cases of Emergency, Combating Pollution of the Mediterranean Sea (January 2002), replacing the Protocol on Barcelona Convention concerning Cooperation in Combating Pollution of the Mediterranean Sea by Oil and Other Harmful Substances in Cases of Emergency (Barcelona 16 February 1976)



It is very interesting to note that a major impulse to incorporate sustainable materials in the development of new satellites is coming from what has been labelled as “ecodesign” ([Design for Innovative Value](#)). In the context of space policies, *ecodesign* would mean that, the approach to the building of satellites and orbiting space facilities should focus on “sustainability by design,” to use a terminology borrowed from the contemporary concept of “privacy by design” (Regulation (EU) 2016/679). The goal of manufacturing sustainable spacecraft is linked to the shaping of policies for deorbiting management. Since sustainable is something that allows a process to endure indefinitely, minimizing or eliminating its negative impact on the environment, then sustainable production implies taking advantage of compostable materials. In this respect, national and international space legislation should place limits to the type and nature of materials to be used in space, by setting a percentage of compostable composition depending on the space item. This would enable de-orbiting only for those (smaller) portions of spacecraft that cannot biodegrade in space.

---

## Ongoing Search for Space Authority

The lack of binding international agreement on space debris is, in particular, related to political and regulatory aspects. Just the absence of an authority for the regulation of space debris creates that gap which results in inability to reach a common agreement at the international level to address such a crucial issue.

The matter needs to be carefully unraveled step by step, starting from fundamental questions that are to be posed: should the above said authority be a new one, explicitly created for this purpose, or should it be an already existing institution appointed? And, if it be an already existing institution, which one? Would it be suitable to promote, drive, and guarantee the legal certainty and standardization, if necessary, coercing states into it, to safeguard the long-term sustainability of outer space activities, and the balanced exploitation of its resources?

During UNISPACE+50, the Committee on the Peaceful Uses of Outer Space (COPUOS) identified seven thematic priorities and evaluated potential initiatives introducing legal mechanisms necessary to achieve the safety and sustainability of space operations. The Chair of the Working Group on the Status and Application of the Five United Nations Treaties on Outer Space noted the lack of exhaustiveness relating to semantic richness of some notions. Actually, there is not one responsible authority for tracking space debris internationally but several ones. The United States does track space debris to protect European satellites, while within Europe some of that information is shared with the rest of the world or within the SST Framework Program. In addition, the Inter-Agency Space Debris Committee (IADC) is an international association involving various space agencies from around the world with the aim of addressing the problem of space debris.

In this regard, the “Space2030” agenda, encouraging a collaboration between the Office for Outer Space Affairs and industry entities, called for efforts aimed at promoting transparency and sustainability of space activities through the pillars of space economy, space diplomacy, and space accessibility. In line with a view to

straighten a space global governance, the General Assembly looked at “Space 2030” as a strategic overview within UNISPACE+50 conference which engaged all key stakeholders in the space arena (A/AC.105/1166).

## **ITU Role in Leading Regulation on Space Debris**

In the current global panorama, the International Telecommunication Union (ITU) could play a role in fostering a common understanding on security challenges in space. Founded in 1865, the ITU is the United Nations agency tasked with allocating “global radio spectrum and satellite orbits, [developing] the technical standards that ensure networks and technologies seamlessly interconnect, and [striving] to improve access to ICTs to underserved communities worldwide.”

When addressing the matter of space debris and de-orbiting, in the recent past and hitherto, the ITU has mostly issued recommendations. One of the most notable recommendations has been, for instance, the December 2010 Recommendation ITU-R S.1003-2, concerning the “Environmental protection of the geostationary-satellite orbit.” In here, the role of the agency comes into play because of the increasing threat posed by spacecraft fragments, resulting in multiplying debris crowding the orbit at stake.

ITU-R S.1003.2 provides guidance about disposal orbits for satellites in the geostationary satellite orbit (GSO). In this orbit, there is an increase in debris due to fragments resulting from increased numbers of satellites and their associated launches. Given the current limitations (primarily specific impulse) of space propulsion systems, it is impractical to retrieve objects from GSO altitudes or to return them to Earth at the end of their operational life. A protected region must therefore be established above, below and around the GSO which defines the nominal orbital regime within which operational satellites will reside and maneuver. To avoid an accumulation of non-functional objects in this region, and the associated increase in population density and potential collision risk that this would lead to, satellites should be maneuvered out of this region at the end of their operational life. In order to ensure that these objects do not present a collision hazard to satellites being injected into GSO, they should be maneuvered to altitudes higher than the GSO region, rather than lower.

The recommendations embodied in ITU-R S.1003.2 are:

- Recommendation 1: As little debris as possible should be released into the GSO region during the placement of a satellite in orbit.
- Recommendation 2: Every reasonable effort should be made to shorten the lifetime of debris in elliptical transfer orbits with the apogees at or near GSO altitude.
- Recommendation 3: Before complete exhaustion of its propellant, a geostationary satellite at the end of its life should be removed from the GSO region such that under the influence of perturbing forces on its trajectory, it would subsequently remain in an orbit with a perigee no less than 200 km above the geostationary altitude.

- Recommendation 4: The transfer to the graveyard orbit removal should be carried out with particular caution in order to avoid radio frequency interference with active satellites. The document, only one of a series in this decade, aims to ensure “the rational, equitable, efficient and economical use of the radio-frequency spectrum by all radiocommunication services, including satellite services, and carry out studies without limit of frequency range on the basis of which Recommendations are adopted,”<sup>3</sup> providing then direction and guidelines to national and international space operators.

By definition though, an act of recommendation is not legally binding, and this explains the “softer” capacity of its provisions. For instance, the one expressed therein, that cites: “before complete exhaustion of its propellant, a geostationary satellite at the end of its life should be removed from the GSO region such that under the influence of perturbing forces on its trajectory, it would subsequently remain in an orbit with a perigee no less than 200 km above the geostationary altitude,” or even “the transfer to the graveyard orbit removal should be carried out with particular caution in order to avoid RF interference with active satellites.”

## **ITU Role in Guaranteeing Space Security Against the Debris Threat**

As mentioned before, one of the duties of the ITU is to oversee the definition of technical standards for the use of radio waves, and so, directly and indirectly, the functioning of, and the proper access to, the interconnection between the ICT infrastructures all around the world. This means that, through one of its three internal sectors, the ITU-R, the assignation of satellite orbits is already part of its statutory activities. Furthermore, since the 1973 ITU Convention, article 33, defined the Geostationary orbit (GEO) as a “limited natural resource” (Hackett 1994), many decades passed, and ITU continued its rationalization attempts of the orbit use for telecommunication purposes, thus shaping, in the form of resolutions and recommendations, an incomparable technical and political legacy that, as extremely valuable is today, even more will be in the future, with additional private operators joining orbits exploitation. As things stand, it would be a natural consequence to just broaden ITU mandatory sphere of action to the debris issue, rather than deferring it in the expectation that, eventually, an agreement over the institution of a new ad hoc regulatory body will be reached soon.

The second reason for believing that ITU would be the most logical option for a leadership role lies in its very structure: in fact, it has the peculiar characteristic of being the sole UN agency to enlist both public and private stakeholders. With its 193 Member States, about 700 tech companies, ICT regulators and leading academic institutions, ITU is perfectly capable of establishing itself as the global funnel for the different stakeholders, and for all space players’ interests. Furthermore, as noted by Antoni et al, “the ITU working groups which are a great example of effective

mechanism to overcome conflicting interests among national authorities, and allow for coordination at international level and the bottom-up development of binding instruments” (Antoni et al. 2020). The efficiency and immediacy of the dialogue between governments and private entities, in particular, would benefit from this choice, and also from the technical asset that the ITU is the bringer and guarantor of.

---

### **Discussion: Fairway Charges in Space, a Starting Point for Space Debris Regulation?**

A last question still remains. How may international law support settling on the ITU as the organization of reference for space debris mitigation rules? Since the dawn of the space era, jurists have examined maritime law to find elements of similarity that facilitate the development of rules for outer space activities. A number of provisions are even similar, both in phrasing and in content (adapted, of course, to the different contexts), with the first one serving as a model for inspiration for the latter. Especially in relation to the high seas discipline, this becomes more evident. Therefore, a study on the applicability of the fairway charges rulebook in space, albeit with some variations, could be the starting point for consistently assuring the efficient use of the spectrum/orbit resource.

In maritime law, the en route rights are governed by the 1972 IMO Convention concerning International regulations for preventing collisions at sea (COLREGs 72), which was drafted and adopted as an updated version of the 1960 Collision regulations. The Convention, and its subsequent amendments, lays down rules on a crucial issue in the maritime environment, that of the naval traffic in the sea, aiming at reducing the risk of collision between vessels, through the introduction of traffic separation schemes, and in particular through the establishment of priorities between routes and actions to be taken, for instance in case of overlapping trajectories.

A parallel drawn between vessels and spacecraft as well as routes and orbits would be an interesting exercise. The latter could indeed bear some interesting outputs, benefitting the management of spacecraft especially in the most crowded orbits afflicted by the increasing presence of debris. Provisions such as the one that cites: “a vessel which was required not to impede the passage of another vessel should take early action to allow sufficient sea room for the safe passage of the other vessel. Such vessel was obliged to fulfil this obligation also when taking avoiding action in accordance with the steering and sailing rules when risk of collision exists” (Rule 9) could shape the basis for an obligation, upon the launching states, to take all possible and preventive action not to impede the passage of other spacecraft in orbit. Extensively, this would result in de-orbiting measures to be mandatorily planned in advance, and set in motion before the spacecraft’s operational life comes to an end, in order to clear the path as required by the rule.

Moreover, Rule 17 of COLREGs 72 states that a stand-on vessel may “take action to avoid collision by her manoeuvre alone as soon as it becomes apparent to her that

the vessel required to keep out of the way is not taking appropriate action in compliance with these Rules.” Transposed for our purposes, that would pose states which command operative spacecraft, risking collision with a “dead” one, on an upper decisional level than the state that owns the latter, broadening the borders of their maneuver power. The same would go with responsibility issues, where Rule 18 “includes requirements for vessels which shall keep out of the way of others.” Indeed, this would open new scenarios as for the framework of international liability and responsibility for damage between two or more launching states, with the rules currently in force being called into question.

---

## Conclusions

By way of conclusion, maritime law can really be a platform where space law can grow. It remains to be seen to what degree, and by what means, the international institutions and operators will want, and be able, to draw on analogies from the same successful maritime role model in space.

In addition, the ITU can be the right reference to contribute to the sustainability of outer space that can be guaranteed from regulation to the support of commercialization. Finally, it is important to create an international consciousness and awareness on the importance of solving debris legal aspects.

---

## References

- Antoni, N., Giannopapa, C., Schrogl, KU (2020) Legal and policy perspectives on civil-military cooperation for the establishment of space traffic management. *Space Policy J*, In press, JSPA\_101373
- Design for Innovative Value. Towards a Sustainable Society: Proceedings of EcoDesign 2011: 7th International Symposium on Environmentally Conscious Design and Inverse Manufacturing BY Mitsutaka Matsumoto, Yasushi Umeda, Keijiro Masui, Shinichi Fukushima, Springer Science & Business Media, 3 Apr 2012
- ESA Safety and Security. [https://www.esa.int/Safety\\_Security/Clean\\_Space/ecodesign](https://www.esa.int/Safety_Security/Clean_Space/ecodesign)
- Guidelines for the long-term sustainability of outer space activities, Committee on the Peaceful Uses of Outer Space, Fifty-ninth session, Vienna, 8-17 June 2016
- Guidelines for the long-term sustainability of outer space activities, Committee on the Peaceful Uses of Outer Space, Sixtieth session, Vienna, 7-16 June 2017
- Hackett GT (1994) *Space Debris and the Corpus Iuris Spatialis*, Forum for Air and Space Law, vol 2. Editions Frontieres
- <http://spacenews.com/op-ed-chinas-well-crafted-counterspace-strategy/>
- [http://www.esa.int/About\\_Us/ECSL\\_European\\_Centre\\_for\\_Space\\_Law/About\\_space\\_law](http://www.esa.int/About_Us/ECSL_European_Centre_for_Space_Law/About_space_law)
- <http://www.imo.org/en/About/Conventions/Pages/Home.aspx>
- [http://www.un.org/depts/los/convention\\_agreements/convention\\_overview\\_convention.htm](http://www.un.org/depts/los/convention_agreements/convention_overview_convention.htm)
- <http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introliability-convention.html>
- <http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/intromoon-agreement.html>

<http://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/introrescueagreement.html>  
[https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg\\_no=XII-1&chapter=12&lang=en](https://treaties.un.org/pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XII-1&chapter=12&lang=en)

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) Thematic priority. 2. Legal regime of outer space and global governance: current and future perspectives, Committee on the Peaceful Uses of Outer Space, Note by the Secretariat, A/AC.105/C.2/2019/TRE/L.1.



# Security Exceptions to the Free Dissemination of Remote Sensing Data: Interactions Between the International, National, and Regional Levels

# 57

Philip De Man

## Contents

Introduction .....	1092
International Level .....	1093
Introduction .....	1093
Scope of Application and Security .....	1095
Free Use and Dissemination .....	1097
Security Limiting Dissemination .....	1098
Security as a National Exception to Principles of International Law .....	1100
National Level .....	1103
Introduction .....	1103
Scope of the SDSA .....	1104
National Security Restrictions in the SDSA .....	1105
Regional Context and the SDSA .....	1108
Regional Level .....	1109
Introduction .....	1109
Copernicus Regulations: Scope .....	1111
Open Access Policy and Security Restrictions .....	1111
Sentinel Data .....	1115
Contributing Mission Data .....	1116
Conclusion .....	1118
References .....	1119

## Abstract

International rules on remote sensing are generally silent on restrictions to remote sensing data dissemination in favor of broadly phrased principles of free collection and exchange of information. At the same time, those States and regional

---

P. De Man (✉)  
University of Sharjah, Sharjah, UAE  
University of Leuven, Leuven, Belgium  
e-mail: [philip.deman@kuleuven.be](mailto:philip.deman@kuleuven.be)

groups that have adopted specific remote sensing legislation typically focus on the security implications of such free data dissemination when applied to sensitive information. This chapter aims to give an overview of the meshwork – at the same time overlapping and partially lacunal – of international, regional, and national rules specifically adopted for the regulation of remote sensing activities, with a view of distilling the general benchmarks of a regime for the dissemination of remote sensing data, and the acceptable limitations for national security concerns. In so doing, the chapter aims to keep a clear focus on specific regulations rather than abstract tendencies. The discussion of every level therefore centers on a legal document deemed particularly emblematic of the regulation of remote sensing at that level. Reflecting this, the chapter is divided into the following sections: (I) the international level, analyzed through the lens of the 1986 United Nations (UN) Remote Sensing Principles; (II) the national level, illustrated by the comprehensive remote sensing regulation in the German Satellite Data Security Act; and (III) the regional level, where the interactions between the international and the national remote sensing rules are exemplified by the regulations of the European Union (EU) on data and information disseminated through the Copernicus program.

---

## Introduction

As a legal matter, checks on the dissemination of remote sensing data for reasons of national security combine issues governed by, *inter alia*, the law on outer space and telecommunications, human rights law, and trade and export control regulations. They also stand at the crossroads of intersecting regulations at the international, national, and regional levels. The laws on outer space and space communications deal with issues that are intrinsically international in nature and their general principles are laid down in a limited set of multilateral conventions and resolutions. These typically focus on the freedom of States to use outer space for activities such as remote sensing, including dissemination of their data. Matters of national security are, by definition, eschewed in multilateral negotiations so as to allow States to retain a high level of discretion for their regulation at the municipal level. It should not be surprising, therefore, that, while international rules on remote sensing are generally silent on restrictions to the free dissemination of remote sensing data, the focus of national regulation lies rather on the security implications of such freedom when applied to sensitive data.

This shift in focus is also due in part to the distinct legal environment in which national legislators operate, where general principles on remote sensing agreed to at the international level must be integrated in an overlapping patchwork of rules on such diverse matters as national licensing of space activities, trade, and export control. In this respect, national export control rules still often focus heavily on trade in satellite technologies and ground control hardware, leaving the dissemination of the collected data to other areas. (See Schmidt-Tedd and Kroymann 2008, 103 and 107; noting that the German Satellite Data Security Act was necessary to close a potential legal loophole in export control regulations, which typically only



apply to satellite technologies but not to the distribution or transfer of data generated by these satellites.) And while States are increasingly active in adopting national space legislation, cases where the dissemination of remote sensing data are explicitly regulated at the domestic level remain rare. Further, the relative novelty of highly detailed remote sensing imagery collected, stored, and disseminated on a large scale by private actors means that, even if specific rules of national space law have been adopted, detailed regulation of the security implications of remote sensing data dissemination may still be missing.

In light of this situation, the present chapter wishes to give an overview of the meshwork – at the same time overlapping and partially lacunal – of international, regional, and national rules specifically adopted for the regulation of remote sensing activities, with a view of distilling the general benchmarks of a regime for the dissemination of remote sensing data, and the acceptable limitations for national security concerns. In so doing, the chapter aims to keep a clear focus on specific regulations rather than abstract tendencies. The discussion of every level therefore centers on a legal document deemed particularly emblematic of the regulation of remote sensing at that level. Reflecting this, the chapter is divided into the following sections: (I) the international level, analyzed through the lens of the 1986 United Nations (UN) Remote Sensing Principles (Principles Relating to Remote Sensing of the Earth from Outer Space, UN Doc. A/RES/41/65 of 3 December 1986 (hereinafter: “Remote Sensing Principles” or “RS Principles”)); (II) the national level, illustrated by the comprehensive remote sensing regulation in the German Satellite Data Security Act (Act to give Protection against the Security Risk to the Federal Republic of Germany by the Dissemination of High-Grade Earth Remote Sensing Data of 23 November 2007, 2590 *Federal Gazette (BGBl.)*, Year 2007, Part I, No. 58, 28 November 2007 (hereinafter: “Satellite Data Security Act” or “SDSA”)); and (III) the regional level, where the interactions between the international and the national remote sensing rules are exemplified by the regulations of the European Union (EU) on data and information disseminated through the Copernicus programme (see, in particular, Commission Delegated Regulation (EU) No. 1159/2013 of 12 July 2013 supplementing Regulation (EU) No. 911/2010 of the European Parliament and of the Council on the European Earth monitoring programme (GMES) by establishing registration and licensing conditions for GMES users and defining criteria for restricting access to GMES dedicated data and GMES service information, *OJ L* 309/1 of 19 November 2013).

---

## International Level

### Introduction

The activity of remote sensing in its broadest form can be defined as any act of gathering information about an object without making physical contact. A more narrow approach, however, defines the notion as the act of collecting and distributing

information about phenomena on Earth with the aid of satellites. As such, it is subject, in the first place, to the rules of international law regulating activities in outer space, in particular the Outer Space Treaty (Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies of 27 January 1967, 610 *UNTS* 8843 (hereinafter: “Outer Space Treaty” or “OST”). The provisions of the Outer Space Treaty avoid any references to the collection of data from outer space, or indeed any other specific type of space activities, in favor of a general set of principles built on the fundamental notion of free exploration and use outer space. However, existing practice at the time of negotiations of the Outer Space Treaty indicates that States generally agreed on the legality of remote sensing activities as non-intrusive means of verification, transparency, and confidence-building. (The US Corona program, aimed at photographing the territory of the former USSR, was launched as early as June 1959 and lasted until 1972. For more on the early days of remote sensing, see Bosc 2015, 557–563.) Despite lacking, therefore, a legal basis explicitly confirming the legality of remote sensing, be it for scientific, commercial, or military reasons, the absence of any specific prohibition of an on-going activity should be taken as an indication that remote sensing is covered, in all its varieties, by the general freedom of States to explore and use outer space in Article I, para. 2 OST. At the same time, the codification in binding language of the principle that outer space is not subject to national appropriation by any means whatsoever in the same convention effectively deprived sensed States from invoking sovereignty as a legal basis for objecting to data collection of their territories from space. (Art. II OST. This distinguishes remote sensing in space law from air law, where the recognition of complete and exclusive sovereignty of States over the airspace above their territory effectively prohibits States from remotely sensing the territories of other States without their permission. See Art. 1 of the Paris Convention relating to the Regulation of Aerial Navigation of 13 October 1919, *Br. Treaty Series* 1923, No. 14; Art. 1 of the Chicago Convention on International Civil Aviation of 7 December 1944, 15 *UNTS* 295. Art. 36 of the Chicago Convention further provides that each contracting State “*may prohibit or regulate the use of photographic apparatus in aircraft over its territory.*”)

Though the activity of placing satellites in an orbit around Earth with the purpose of collecting, for military reasons or other, data about the territories of States and areas outside national jurisdiction, was hence accepted, the related issue of the processing and dissemination of the data collected in that process continued to raise sensitive questions rooted in sovereignty and national interests. After a lengthy process of negotiation, marked by disagreement over both content and form, the Legal Subcommittee (LSC) and the plenary Committee on the Peaceful Uses of Outer Space (COPUOS) finally reached consensus on 15 Principles Relating to Remote Sensing of the Earth from Outer Space, which were subsequently adopted, also by consensus, by the UN General Assembly (UNGA) in 1986. (The item on remote sensing was first introduced in the agenda of the LSC in 1972: see Report of the Legal Sub-Committee on the Work of its Eleventh Session (10 April–5 May 1972), UN Doc. A/AC.105.101 of 11 May 1972, 3, agenda item 4 (c). For the history of the negotiations of the RS Principles, see Smith and Reynders 2015, 86–87) The

discussions mainly centered on the legal form of the document and the extent of the application of the accepted principle of States' permanent sovereignty over natural resources to data about these resources, and pitched developed countries against developing countries on issues of prior consent and exclusive access. (See the UNGA Resolutions concerning Concerted Action for Economic Development of Economically Less Developed Countries, UN Doc. A/RES/1515 (XV) of 15 December 1960, and Permanent Sovereignty over Natural Resources, UN Doc. A/RES/1803 (XVII) of 14 December 1962.) Though ambiguous at points in their formulation and nonbinding in nature, the 1986 Principles were successful in ending a laborious process of negotiations and consultations by consensus, and as such should be the first stop in any analysis aiming to clarify the limits, if any, to remote sensing data collection and dissemination on security grounds.

### Scope of Application and Security

One of the main points of contention that arose during the negotiations for the RS Principles concerned the scope of application of the 15 principles. As noted, remote sensing is not necessarily restricted to data collection of Earth from space, and different States had different ambitions for the instrument they were negotiating. Ultimately, the RS Principles Resolution defines its own scope of application both narrowly and broadly, in that it only applies to remote sensing of the Earth from outer space when performed for certain purposes, while including all phases of the data collection and dissemination process in the definition of these activities. As such, the RS Principles provides that the term "remote sensing activities," when used in the document, refers to "*the operation of remote sensing space systems, primary data collection and storage stations, and activities in processing, interpreting and disseminating the processed data.*" (Principle I (e). According to Principle I (b), (c), and (d), "primary data" "*means those raw data that are acquired by remote sensors borne by a space object and that are transmitted or delivered to the ground from space by telemetry in the form of electromagnetic signals, by photographic film, magnetic tape or any other means; ['processed data'] means the products resulting from the processing of the primary data, needed to make such data usable; [and 'analysed information'] means the information resulting from the interpretation of processed data, inputs of data and knowledge from other sources.*") However, the term "remote sensing" in this definition exclusively refers to "*the sensing of the Earth's surface from space by making use of the properties of electromagnetic waves emitted, reflected or diffracted by the sensed objects, for the purpose of improving natural resources management, land use and the protection of the environment [...]*" (Principle I (a) RS Principles).

If the peculiar approach to delineate the scope of the RS Principles appears to undercut its relevance for the purpose of space security, a proper understanding of the document's genesis and the nature of remote sensing will suffice to reject this notion. The fact that the instrument defines the term "remote sensing" only with respect to natural resource management, land use, and the protection of the

environment does not mean that the activity of remote sensing may only be performed for these three purposes, and that remote data collection of other State's territories for other aims such as security would be disallowed under international law. As the phrase "for the purpose of these principles" makes clear, the only implication of the definition as provided is that the 1986 Resolution will simply not, as such, apply to remote sensing activities performed for reasons other than those listed in the definition. (Compare Lee 2001, considering this a "creative" interpretation, though ultimately appearing to argue in favor of it.) Indeed, the definition of the term "remote sensing" in the RS Principles merely reflects the primary concerns of the States gathered to negotiate a principles document in a forum – COPUOS – that eschews discussions on national security interests and military activities in favor of principles of a general application or, in this case, tailored to natural resource management and related purposes. The definition should also be read against the background of the Outer Space Treaty, which does not distinguish in the formulation of its principle of free exploration and use between activities performed for military or other purposes.

The above does not mean that the RS Principles have no legal implications for remote sensing activities performed for military reasons, for two reasons. First, it will often be difficult to determine, in practice, whether a remote sensing activity is solely carried out for one or more of the purposes mentioned in the 1986 Resolution due to the inherently dual-use nature of many remote sensing satellite activities. The GMES programme on Global Monitoring for Environment and Security, developed jointly by the European Union and the European Space Agency and later renamed Copernicus, is a prominent example of a remote sensing project set up for purposes that, at the same time, fall within and outside of the scope of the RS Principles (see section "[Copernicus Regulations: Scope](#)" on Copernicus). Further, even when a program as such was not originally set up "for the purpose of" dual-use, data collected by satellites through purely civilian programs may also be used for military purposes, while conversely remote sensing operations of the military may result in civilian applications for the management of natural resources.

At this point, the RS Principles' narrow definition of "remote sensing" must be read in conjunction with the instrument's broad approach to "remote sensing activities." As noted, the latter concept includes the operation of space systems and the collection and storage of primary data, as well as activities in the processing, interpretation, and dissemination of such data. The sweeping nature of data collected by modern remote sensing activities means that it is often only at the stage of analyzing and interpreting the collected data with the aim of using and disseminating them that the nature of the activity may be classified as either for security or other purposes. It follows from a good faith interpretation of the RS Principles that they will need to be taken into account for the regulation of remote sensing activities whose design or implications combine one or more of the three purposes covered by the definition of "remote sensing" in the Principles with other purposes, including security, at least as far as the phase of data collection, storage, and, possibly, processing is concerned. It is only when the data collected is then analyzed,

interpreted, and disseminated for purely security purposes that the activity would arguably no longer be covered by the RS Principles.

Secondly, and more importantly for the present chapter, it is not because a program of remote sensing is performed solely for the purpose of one of the three goals enshrined in Principle I (a) of the 1986 Resolution, and that the processed data and analyzed information following from that program is only in fact used for civilian purposes, that their dissemination would necessarily be bereft of any security implications. Such dissemination is undoubtedly and even under the strictest interpretations of the definitions of “remote sensing” and “remote sensing activities” covered by the RS Resolution. Hence, it is clear that an answer to the question of the precarious balance between free access to and dissemination of data and information collected by remote sensing programs for civilian purposes, and restrictions thereto for reasons of national security, will at least in part depend on the content of the RS Principles. The answer will ultimately remain ambiguous, however, for the principles, while acknowledging the freedom to use outer space for the purpose of remote sensing, are silent on considerations of national security that may limit this freedom.

## Free Use and Dissemination

Though the preamble of the Remote Sensing Principles does not explicitly refer to the Outer Space Treaty, its contents are clearly inspired by this convention. As such, the Principles are founded, in the first place, on the freedom of States to operate remote sensing satellite systems, and freely store, process, interpret, and disseminate data collected in the process (Achilleas 2008, 2). This follows from a combined reading of the definition of “remote sensing activities” in the 1986 Resolution with the explicit reformulation of and reference to Article I OST in its Principles II and IV. The latter Principle confirms the legality of remote sensing activities by noting that they “*shall be conducted in accordance with the principles contained in [Article I OST], which, in particular, provides that the exploration and use of outer space shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic or scientific development, and stipulates the principle of freedom of exploration and use of outer space on the basis of equality.*” Principle II paraphrases the remaining paragraph of Article I OST by providing that “[r]emote sensing activities shall be carried out for the benefit and in the interests of all countries, irrespective of their degree of economic, social or scientific and technological development.” To placate the developing countries, the Principle adds that the needs of these States must be taken “*into particular consideration,*” without, however, identifying specific ways, including limitations to the above freedom, in which this should be done.

Other principles echo different provisions of the Outer Space Treaty. Principle III of the RS Resolution restates and clarifies Article III OST by requiring that remote sensing activities shall be conducted “*in accordance with international law, including the Charter of the United Nations, the [Outer Space Treaty], and the relevant instruments of the International Telecommunication Union.*” Principle XIV is

notable as well, for it confirms the application of Article VI OST to “*States operating remote sensing satellites,*” which shall hence assure that their activities, even when performed by nongovernmental entities, “*are conducted in accordance with [the RS Resolution] and the norms of international law.*” Commercial owners and operators of remote sensing satellite systems must hence also abide by all applicable rules of international law by virtue of their State’s responsibility for their activities. The reference in this context to “norms of international law” appears to expand the text of Article VI OST, which only refers to the “*provisions set forth in the [Outer Space Treaty],*” but ultimately is the logical result of a combined reading of this provision with Article III OST. More notable is that the phrasing of Principle XIV, in apparent deviation from the general scope of the RS Principles, only confirms the international responsibility under Article VI OST for the activities of “*States operating remote sensing satellites,*” rather than States performing “remote sensing activities.” When read in conjunction with the requirement of authorization and continuing supervision by States of the activities of their nationals, Principle XIV could thus be interpreted restrictively as merely confirming the international responsibility of States for the operation, by nongovernmental entities, of remote sensing space systems, but not for the other aspects of the remote sensing activity as defined in the 1986 Resolution, i.e., the collection and storage of primary data and, crucially, the dissemination of the data resulting therefrom (compare Mantl 2015, 177–178). Regardless of this interpretation, however, States in their national laws will often go further and also require their remote sensing data providers to obtain permits for disseminating data, at which point a sensitivity check for reasons national security will be performed. (See *infra* on the German Satellite Data Security Act of 2007. It could be argued that States would still be responsible for the dissemination of data collected from remote sensing operations of their nationals under Art. VI OST, for that provision more generally refers to “national activities in outer space” and “the activities of non-governmental entities in outer space.” However, such argument would rest on the extension of the broad definition of “remote sensing activities” in the RS Principles to the term “(national) space activity” in the Outer Space Treaty, which should not necessarily be accepted, in particular taking into account Principle XIV of the RS Principles.)

## **Security Limiting Dissemination**

If the RS Principles clearly confirm the freedom of States to sense the Earth from space and store, process, and disseminate the data and information thus gathered, the instrument is less outspoken on the possible limitations to this freedom, for reasons of national security or other. The main provision aimed at harmonizing the positions of developed and developing States in this respect can be found in Principle IV, the latter part of which provides that remote sensing activities “*shall be conducted on the basis of respect for the principle of full and permanent sovereignty of all States and peoples over their own wealth and natural resources, with due regard to the rights and interests, in accordance with international law, of other States and entities under*

*their jurisdiction.*” The specific phrasing – “, *which*” instead of “, *and which*” – suggests that the obligation of due regard for the rights and interests of other States and entities under their jurisdiction is limited, in the first place, to the context of States’ and peoples’ wealth and natural resources. However, the provision complements this by adding that “[*s*]uch activities shall not be conducted in a manner detrimental to the legitimate rights and interests of the sensed State,” thus requiring that the general rights and interests of other States be taken into account in the performance of remote sensing activities as covered by the RS Principles.

As Principle IV applies to “remote sensing activities,” all aspects of such activities, including the dissemination of stored and processed data and information, may find limitations in the legitimate rights and interests of the sensed State. Principle XII expands on these rights of the sensed State specifically as regards its rights of access to data and information collected through remote sensing. According to this Principle, the sensed States shall have access to “*primary data and processed data concerning the territory under its jurisdiction,*” as soon as they are produced and “*on a non-discriminatory basis and on reasonable cost terms.*” In addition, the sensed States shall have access to “*available analysed information concerning the territory under its jurisdiction in the possession of any State participating in remote sensing activities on the same basis and terms, taking particularly into account the needs and interests of the developing countries.*” While Principle XII focuses on the rights of the sensed State, its provisions are grounded in assumptions of free access to and dissemination of data and information obtained by the sensing State or its nationals. The requirement to make primary and processed data available to the sensed State on a nondiscriminatory and reasonable cost basis implies that, in general, such data must be freely – though not *gratis* – accessible to everyone.

Principle XII could be interpreted as allowing some exceptions to the free dissemination of remote sensing information, as it explicitly requires sensing States to grant the sensed State access to processed information when “available” only. Though the security implications of remote sensing were undoubtedly well-known at the time of negotiation of the RS Principles, the text does not clarify how the availability of processed information may be restricted, and if the justifications for such restrictions could include reasons of national security. And, as noted, the Principles do contain a similar qualification when regulating the access to primary and processed remote sensing data. All of this should perhaps not be too surprising, since, during the negotiations of the 1986 Resolution, only classified military and intelligence-service satellites specifically developed for the purpose of government security applications were able to produce sufficiently high-quality data so as to have possible security implications. Access to these data was already closely regulated on the basis of specific governmental laws and policies. Hence, the principle of the free exploration and use of outer space could easily be confirmed as applying to all aspects of remote sensing activities in a document that, in any case, only addressed such activities for specific nonmilitary purposes.

This is not to say that the end result is satisfactory, or that the historic circumstances surrounding the conclusion of the Principles Resolution should necessarily have resulted in a text that leaves it to the reader to determine what exactly is the

balance between the right of free access to and dissemination of remote sensing data, and limitations for reasons of national security. Compare, for example, the ambiguity of the 1986 Resolution in this respect with the provisions of the 1978 Convention on the Transfer and Use of Data of Remote Sensing of the Earth from Outer Space. (Adapted 19 May 1978, entered into force 21 August 1979. The text of the Convention is annexed to a letter of the USSR representative to the UN Secretary-General dated 28 June 1978, UN. Doc. A/33/162 of 29 June 1978.) Sponsored by the then USSR, the treaty entered into force a year later and was ratified by eight States. (These States are/were Cuba, Czechoslovakia, the German Democratic Republic, Hungary, Mongolia, Poland, Romania, and the USSR.) Even though the Convention is hence of limited legal relevance, it is noteworthy for the limitations it imposes on the distribution of potentially sensitive remote sensing data. In particular, we may refer to Article IV of the Convention, which provides that “[a] Contracting Party in possession of initial data of the remote sensing of the Earth from outer space, with a better than 50 metres resolution on the terrain, relating to the territory of another Contracting Party, shall not disclose or make them available to anyone except with an explicit consent thereto of the Contracting Party to which the sensed territories belong, nor shall it use them or any other data in any way to the detriment of that Contracting Party.” While the 1978 Convention has, for all intents and purposes, passed into disuse, its approach has been partially replicated in national laws on remote sensing where they explicitly allow for limitations on the access to remote sensing data when its resolution is sufficiently high so as to potentially reveal information that may affect the State’s national security. (See, for example, the Annex to EU Regulation 1159/2013).

## Security as a National Exception to Principles of International Law

The manifest focus of the 1986 Principles on the free access to and dissemination of data gathered through remote sensing could raise the issue of conformity with this international instrument of such national security exceptions (see Lyall and Larsen 2009, 424–425). To be sure, the question may be of limited importance, since UNGA resolutions are legally nonbinding documents, and the formulation of the 1986 Principles as they have been adopted leaves ample discretion for States to implement its provisions in such a manner as they see fit. Nevertheless, it is commonly accepted that the Principles on Remote Sensing set an important legal precedent since they successfully managed to end years of negotiations in the form of a text that was adopted with consensus at all stages. More importantly, the principles are generally followed in State practice, even to the extent that they are sometimes believed to either declare or have become, at least in part, norms of customary international law. (See Answers from the Chair of the Space Law Committee of the International Law Association (ILA) to questions by the Chair of the Working Group of the LSC, UN Doc. A/AC.105/C.2/2015/CRP.25 of 22 April 2015: “[u]nlike the OST, the ‘Principles Relating to Remote Sensing of the Earth from Outer Space’ is a non-binding instrument except when declaring customary



*international law.*” The Chair opines in this regard that Principle XIV of the 1986 Resolution addressing international responsibility is not of customary nature, for “[t]his Principle would be confining the scope of Article VI of the OST to ‘states operating remote sensing activities’” (with reference to Cheng 1997, 572–597.) Whether national security exceptions in domestic laws are, then, in conformity with the 1986 Resolution depends as much on the interpretation of the latter document as on the uniformity of State practice that allows for exceptions in the name of national security. (The consistent inclusion of these exceptions in the national policies and laws of some of the most important spacefaring States has even prompted some to argue that the national security exception in turn could be considered a rule of CIL itself. See De Beer, June 2015.)

While the latter issue will be dealt with later on in this chapter, the matter of interpretation of the RS Principles as allowing, or not, restrictions on the access to and dissemination of information for reasons of national security should be answered in the affirmative. As noted, Principle IV requires that remote sensing activities “*shall not be conducted in a manner detrimental to the legitimate rights and interests of the sensed State.*” To the extent that the dissemination of remote sensing data and information is considered an activity subject to authorization under international space law, UNGA Resolution 68/74 of 2013 confirms that national security concerns may be taken into consideration in the implementation of this international principle (Recommendations on National Legislation relevant to the Peaceful Exploration and Use of Outer Space, UN Doc. A/RES/68/74 of 11 December 2013). The resolution confirms that the conditions for such authorization “*should be consistent with the international obligations of States, in particular under the United Nations treaties on outer space, and with other relevant instruments, and may reflect the national security and foreign policy interests of States*” (Paragraph 4 of the Resolution). Principle III, mirroring Art. III OST, also notes that remote sensing activities shall be performed in accordance with international law, in particular the Charter of the United Nations and the relevant instruments of the International Telecommunication Union (ITU). International law commonly accepts national security interests as “*legitimate rights and interests,*” which should thus be taken into account by other States in their remote sensing activities. Moreover, such interests are also generally accepted exceptions to the fundamental freedom of information, as widely codified in both universally and regionally applicable instruments on human rights (see Achilleas 2001). Article 19 of the International Covenant on Civil and Political Rights (adapted 16 December 1966, 999 UNTS 171) defines the freedom of expression as the freedom of everyone to “*seek, receive and impart information and ideas of all kinds, regardless of frontiers, either orally, in writing or in print, in the form of art, or through any other media of his choice.*” While this right may hence be invoked to receive and impart remote sensing data and information, it is subject to restrictions when these are “*provided for by law and are necessary [. . .] [f]or the protection of national security or of public order (ordre public), or of public health or morals.*” (See further Art. 19 of the Universal Declaration of Human Rights, UN Doc. A/RES/217A (III) of 10 December 1948. For codifications of this right and security exceptions thereto at the regional level, see Art. 10 of the Convention for the

Protection of Human Rights and Fundamental Freedoms of 4 November 1950, 213 *UNTS* 222; Art. 13 of the American Convention on Human Rights of 22 November 1969, 1141 *UNTS* 123; Art. 9 of the African Charter on Human Rights and Peoples' Rights of 27 June 1981, 1520 *UNTS* 217.) Similar exceptions grounded in concerns for national security are recognized in the provisions of the ITU Constitution on the public's right to correspond through telecommunications as well. (While the ITU Constitution – a binding treaty ratified by 193 States – recognizes the right of the public to correspond by means of the international service of public correspondence, its “*Member States also reserve the right to cut off, in accordance with their national law, any [...] private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency.*” See Arts. 33 and 34 (2) of the Constitution and Convention of the International Telecommunication Union, most recently amended in 2018, published in the Basic Texts of the ITU, 2019.)

States may, thus, according to international law, restrict access to data collected through remote sensing for reasons of public security in their national legislation. Even if the RS Principles do not explicitly contain a provision in this regard, their general phrasing leaves room for discretion by States when promulgating domestic regulations on remote sensing, as is indeed confirmed by other, binding sources of international law on human rights and telecommunications. (It has been argued that States that do not provide for checks on the dissemination of remote sensing data would violate their obligations under Article VI OST: see Schmidt-Tedd and Kroymann 2008, 105. As noted, this argument relies on an extension of the definition of “remote sensing activities” of the RS Principles to the Outer Space Treaty.) Still, States are not granted unfettered discretion to determine at will the grounds for and means of restricting access to remote sensing data and information. International human rights and telecommunications law are adamant that exceptions to the freedom of expression are applied restrictively, and are only allowed when provided for by law, and when they are actually necessary to protect national security. Likewise, the RS Principles insist that the rights and interests of States must be legitimate in order to be taken into account by other States. Whether national laws conform to these requirements will depend on how the national security exception is phrased, and what actions authorities may take to safeguard these interests.

In the end, we shall see that most national laws providing for national security exceptions are clearly in line with the Principles and, indeed, have been inspired by the 1986 instrument (see section National Security Restrictions in the SDSA). (See the discussion of the applicable French and German laws in, respectively, Achilleas 2008, 2; Schmidt-Tedd and Kroymann 2008, 104–105.) Moreover, regulatory frameworks governing the access to remote sensing data at the regional level also confirm the importance of the RS Principles, which, in turn, encourage States to provide for the establishment and operation of data collecting and storage stations and processing and interpretation facilities, “*in particular within the framework of regional agreements or arrangements wherever feasible*” (see section Regional Level) (Principle VI).

## National Level

### Introduction

Despite a steep rise in recent years in the number of States that have adopted domestic space legislation, many countries active in space are still lacking a general space law framework. (For an overview of national regulatory frameworks for space activities, see the UN national space law collection at <http://www.unoosa.org/oosa/en/ourwork/spacelaw/nationalspacelaw/index.html>. See also the Space Legaltech platform of the French Sirius Chair, which provides an interactive overview of a much larger cross-section of national space legislation across the world: <http://spacelegaltech.chaire-sirius.eu/>.) Further, most national space laws that have been adopted focus on the authorization and supervision of national space activities in general, without touching on issues of remote sensing, or the dissemination of sensitive data and information collected by private commercial actors in this sector. To the extent that they are not covered by national rules in related fields such as export control, it follows that, for these countries, the collection and distribution of remote sensing data remain mainly regulated by international space and telecommunication law, if at all (Achilleas 2008, 4).

Those States that have promulgated rules on access to remote sensing data and information typically include provisions allowing for the restriction of access to and dissemination of data collected from remote sensing satellites and/or the information derived therefrom. Canada subjects licenses to operate remote sensing space systems to a sensitivity check designed to safeguard the national security interests and international obligations of Canada. (Act Governing the Operation of Remote Sensing Space Systems, Bill C-25 of 25 November 2005. Art. 8 (1) of the Act provides that “*the Minister may, having regard to national security, the defence of Canada, the safety of Canadian Forces, Canada’s conduct of international relations, Canada’s international obligations and any prescribed factors, (a) issue a provisional approval of a licence application; (b) issue a licence; or (c) amend or renew a licence.*” Such license may be suspended and subsequently cancelled if the continued operation of the licensed system would be injurious to these same interests or inconsistent with Canada’s international obligations (Arts. 11 (1) and 12 of the Act). For the purposes of the Act, a remote sensing space “system” includes “*the facilities used to receive, store, process or distribute raw data from the satellites, even after the satellites themselves are no longer in operation*” (Art. 2).) Likewise, Title 51 of the US Code requires that licensees of private remote sensing space systems shall “*operate the system in such manner as to preserve the national security of the United States and to observe the international obligations of the United States*” (51 US Code Subchapter III – Licensing of Private Remote Sensing Space Systems, § 60122). The French Law on Space Operations requires remote sensing data providers to submit a declaration of their activities to the relevant administrative authorities, who must then verify that these activities do not damage the “fundamental interests of the nation,” including in particular the national defense, foreign relations and international obligations of France. (Articles 23, para. 1 and 24, para. 1

of the Loi Relative aux Opérations Spatiales, N° 2008518, 3 June 2008, as most recently amended on 30 May 2013, at <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEXT000018939303>. For a discussion of these provisions, see Achilleas 2008, 7–9.)

While most of these national laws provide only for a general basis for limiting space remote sensing operations for reasons of national security, foreign relations, or international obligations of the State, the actual regulation is left to the relevant authorities to decide at policy level. (Some States have only adopted remote sensing policies, without any specific legal basis. See, for example, the Indian Remote Sensing Data Policy of 2011, RSDP-01:2001, at [https://nrsc.gov.in/Remote\\_Sensing\\_Data\\_Policy](https://nrsc.gov.in/Remote_Sensing_Data_Policy). According to the RSDP, the Government of India reserves the general right to impose control over imaging tasks and the distribution of data from Indian remote sensing satellites when it is of the opinion that national security, the international obligations or the foreign policies of India so require.) Two recent exceptions are the German and Japanese laws dealing specifically with the security implications of remote sensing data. In 2016, Japan adopted the Act on Securing Proper Handling of Satellite Remote Sensing Records, according to which the Prime Minister can prohibit transfer of particular remote sensing data for a limited time if it is necessary for national security (Art. 19 of Act No. 77 of 2016, available with English translation at [https://www8.cao.go.jp/space/english/rs/rs\\_act.pdf](https://www8.cao.go.jp/space/english/rs/rs_act.pdf)). Nine years prior to that, Germany promulgated the 2007 Act to give Protection against the Security Risk to the Federal Republic of Germany by the Dissemination of High-Grade Remote Sensing Data (Satellite Data Security Act, SDSA). Unlike its Japanese counterpart, the Satellite Data Security Act law did not complement a general national space law framework, as it constituted the first foray of the German legislator in space law regulation. (The Japanese Remote Sensing Records Act complements the country's 2008 Basic Space Law, which does not address remote sensing data handling as such: Act No. 43 of 28 May 2008, with unofficial English translation in 34 *J. Space L.* 2008, 471. On this law and its relevance for remote sensing, see Aoki 2010.) As a result, the Act takes a comprehensive approach that touches upon various aspects of the space activity of remote sensing, specifically addressed from a national security perspective.

## Scope of the SDSA

In the preparation for the 2007 Satellite Data Security Act, the UN Principles on Remote Sensing were actively taken into consideration as “*the guiding principle for the practice of Earth remote sensing*” (Schmidt-Tedd and Kroymann 2008, 105). As an Act adopted by a key Member State of the European Union, the European Space Agency and NATO, the SDSA provisions are also careful to take into account the regional context. The Act is thus a uniquely useful tool for assessing the interactions between the regulations on remote sensing data dissemination at the national, international, and regional level. Like the Remote Sensing Principles, the SDSA applies both to the operation of high-grade Earth remote sensing systems and to the

handling of data generated by such systems, until their moment of dissemination (§ 1, (1), 1 and 2 SDSA). Such data include the signals from satellite sensors as well as “*all products derived from the same, regardless of their degree of processing and their type of storage or representation*” (§ 2, (1), 2 SDSA). While the Act thus does not allow for a distinction between primary data, processed data and analyzed information, its overall scope matches the broad definition of the RS Principles’ approach to “remote sensing activities,” though for different objectives.

The SDSA also mirrors the UN Principles on Remote Sensing by excluding the application of the Act to military remote sensing activities, though the exception is phrased more narrowly and conditional upon actual protection of the information generated by such military activities. As such, the SDSA does not limit its scope of application to remote sensing operations undertaken for specific types of civilian purposes, but only excludes its application for “*the operation of high-grade earth remote sensing systems by a State agency with military or intelligence duties, provided that the possibility of unauthorized third parties gaining knowledge of the generated data is excluded*” (§ 1, (2) SDSA). Should the applicable legal framework or the specific contractual provisions for the operation of military remote sensing systems not meet this condition, the SDSA will remain applicable, regardless of the non-civilian nature of the activity. This discrepancy between the SDSA and the RS Principles may be explained by the different objectives of the two regulations – general principles on remote sensing versus security restrictions – and the need to fit the German Act into the existing patchwork of domestic laws, including export control regulations.

## National Security Restrictions in the SDSA

As a domestic act concerned with the national security implications of remote sensing data for Germany, the Satellite Data Security Act naturally restricts its application to remote sensing activities having a clear link with Germany. For the handling of data, such link is established when the dissemination is done by German nationals or foreign legal persons with their head office in Germany, or when the data are disseminated from within the territory of Germany (§ 1, (1), 1 and 2 SDSA). The Act defines a “data provider” as any person who disseminates data generated by a high-grade Earth remote sensing system but limits “dissemination” to the initial act of “*bringing data into circulation or making data accessible to third parties*” (§ 2, (1), 3 and 6 SDSA). Hence, the SDSA only applies to initial data providers but not to remote sensing service providers or data resellers (Schmidt-Tedd and Kroymann 2008, 108). Moreover, such dissemination may only be subject to restrictions for security reasons if the data has a particularly high information content (§ 2, (1), 4 SDSA).

The determination of what exactly constitutes “particularly high information content” is left to the discretion of the Federal Ministry of Economics and Technology (§ 2, (2) SDSA). However, the conditions under which this determination is to be made are specified in the SDSA, in a provision that combines technical data with

security considerations. As such, the information content of remote sensing data shall be determined not only according to the geometric, spectral, radiometric, and temporal resolution but also taking into consideration “*the possible effects of disseminating data with particularly high information content on the vital security interests of the Federal Republic of Germany, the peaceful co-existence of nations and the foreign relations of the Federal Republic of Germany*” (ibid.). For this reason, data providers wishing to distribute high information content data must apply for a dissemination license subject to conditions of reliability, and technical and operational measures to prevent unauthorized persons from gaining access to the installations for receiving, processing, or storing this data (§ 11, (1) and § 12, (1), 1 and 2 SDSA). Such dissemination license is separate from the license that the operator of a high-grade Earth remote sensing system must obtain under the SDSA (§ 3, (1) SDSA).

The SDSA thus takes national security interest into account for the determination of its scope, to the extent that the “particularly high information content” of generated data to which the Act applies must be assessed in light of their potential security sensitivity. However, the initial categorization of data as having particularly high information content is, as such, not a sufficient ground for restricting its dissemination by data providers. The SDSA imposes a double sensitivity check, to be performed by the data provider as well as the relevant authority, before high-grade data is disseminated, in a two-step process. First, data providers that receive a request for dissemination of data that falls under the Act have to perform a sensitivity check, taking into account not only the information content itself but also the represented target area, the ground segment, and the time between the data generation and possible dissemination (§ 17, (1) and (2) SDSA). The actual information content of data is thus but one factor that determines its sensitive nature, which rather follows from a combination of the information about a certain area and the timing of dissemination. (Schmidt-Tedd and Kroymann 2008, 107. See also *infra*, Art. 14 (1) (b) Regulation 1159/2013, according to which the sensitivity of remote sensing information shall be assessed based, *inter alia*, on the time between acquisition of inputs and dissemination of the information.)

It is only when the above factors combined reveal the possibility of harm being caused to the security interests of Germany as defined earlier, that a request for the dissemination of data shall be deemed sensitive. If the request is sensitive, the data provider is prohibited from complying, unless a dissemination permit is obtained, separate from the dissemination license noted earlier. Such permit must also be obtained if the data providers wishes to disseminate high information content data without a preceding request (§ 19, (1) SDSA). Such permit will only be granted if the dissemination of data “*in the individual case does not harm*” the vital security interests of Germany, does not disturb the peaceful co-existence of nations and does not substantially impair the foreign relations of Germany (§ 19, (2) SDSA). If this sensitivity check is not passed the authority may deny the request, or grant a permit on the condition that the request is altered, e.g., by ordering that the resolution is lowered or by imposing a time delay on the dissemination (Schmidt-Tedd and Kroymann 2008, 110). Moreover, the authorities may take other, proportionate measures against a data provider “*in the individual case to ensure the due*

*performance of its obligations,*” in particular by requiring that the dissemination of data to be adapted to the state of the art, or temporarily prohibiting the dissemination of data (§ 16 SDSA).

Though approaching the issue from a different angle, the actual provisions of the German Satellite Data Security Act confirm the UN Principles on Remote Sensing, both in their restrictive approach to imposing limitations on the free dissemination of data, and in the close circumscription of the justifications for such limitations in considerations of international peace and security. First, the SDSA implicitly confirms the principle of free use of outer space through remote sensing activities, including the free and nondiscriminatory dissemination of data therefrom, by requiring that a comprehensive sensitivity check is performed on a case-by-case basis at various intervals by different actors based on a variety of factors, rather than concluding from the general high information content nature of data gathered by a remote sensing program that its dissemination should always be restricted. In also requiring a dissemination license and a separate permit for the dissemination of individual sensitive data, the SDSA goes further than the RS Principles, by extending the authorization and continuing supervision from the operation of the remote sensing system to all aspects of the remote sensing activity as defined in the latter document. Finally, the restrictive and typically temporary measures that authorities can take when national security interests may be compromised indirectly confirms the basic principle of free data dissemination. (Other rules support this as well: see, for example, § 20 of the SDSA, allowing for the granting of collective permits for data dissemination, even if such permits are still subject to strict limits and conditions.)

Second, the careful manner in which the security interests are phrased is clearly in line with the limits to the free dissemination of data contained in Principles III and IV of the 1986 Resolution. Mindful of their exceptional nature, the security grounds in the SDSA have been closely circumscribed as justifying limits to the dissemination of remote sensing data only when they could damage the *vital* security interests of Germany or *substantially* impair the State’s foreign relations. These qualifications ensure that the exceptions are in line with the limits to remote sensing implied by the obligation to have due regard for the legitimate rights and interests of States (see Schmidt-Tedd and Kroymann 2008, 105 (“*fully in line with the inherent limits of remote sensing and the rights resulting therefrom*”)). The third and final ground for limiting the free access to remote sensing data under the SDSA, the peaceful co-existence of nations, undoubtedly conforms to the limits of general international law as applicable by virtue of Principle III of the RS Resolution. As noted, this Principle requires that remote sensing activities shall be conducted in accordance with international law, in particular the Charter of the United Nations. Article III OST adds to this that such application of norms of international law must be “*in the interest of maintaining international peace and security and promoting international cooperation and understanding.*” The peaceful co-existence of nations is an obvious restatement of this fundamental concern of international law, and national exceptions to the free dissemination of remote sensing data are thus clearly in line with the limits of international law as incorporated in Principle III RS Principles and Article III OST.

## Regional Context and the SDSA

The Satellite Data Security Act is overall very conscious of the regional and international security context in which it is to operate. This context is taken into account, in the first place, at the stage of application of the Satellite Data Security Act, which should be excluded when the laws of other countries already apply that are comparable to the provisions and protected interests of the Act. Though mainly concerned with avoiding unnecessary duplication of substantively similar regulations, the grounds for exclusion also take into account the strategic partnerships of Germany, by differentiating between the laws of the Member States of the European Union and third countries. As such, the SDSA provides that it “*may not be applied*” to the operation of a high-grade earth remote sensing system that is permitted under the applicable law of another EU Member State with substantively comparable provisions (§ 1, (2) SDSA). However, the responsible authority “*may waive the application of the Act*” if the legal provisions of a third country satisfy these same requirements and if there is an international treaty between Germany and this third country that affirms the comparability of the provisions and protected interests. (Ibid. This disparity may also be explained by requirements of internal EU law, which aims to eliminate as much as possible any obstructions to the free exchange of information between its Member States. See in this regard also the preamble to EU Regulation 1159/2013, which provides that “*GMES data and information policy should [...] respect the rights and principles recognized in the Charter of Fundamental Rights of the EU, in particular [...] the freedom to conduct business.*”)

The regional and international context is also taken into account in the performance of the sensitivity check for data whose dissemination has been requested. In performing this test, the administrative authority must take into account, inter alia, “*the obligations assumed and agreements entered into by [Germany] with the Member States of the European Union, the parties to the North Atlantic Treaty of April 4, 1949, [...] and Australia, Japan, New Zealand and Switzerland, [as well as] the existing rules under which the requesting party could further transmit the data and the availability of comparable data on international markets*” (§ 17, (3) SDSA). Through this provision, the regional interests of allies are integrated in the sensitivity check to be performed by the national authority under the SDSA. Moreover, the Act also requires, in general, that the personal characteristics of the requesting party must be taken into account when performing a sensitivity check (§ 17, (2) SDSA). It follows that requests for information by EU and NATO Member States will typically not be deemed sensitive. (Schmidt-Tedd and Kroymann 2008, 113: “[*a*]s a result [*of the criteria for the sensitivity check*], data requests of NATO member states will not be sensitive in most instances.”) However, the interests of regional partners or allies are still not grounds for a blanket denial *c.q.* approval of requests to disseminate remote sensing data, as they are only one of many factors to be taken into account in an individualized security test.



Finally, it may be added that security interests and regional alliances are not only justifications for restrictions on the free dissemination of remote sensing data but are also taken into account by the German legislator as grounds for priority treatment of requests for such dissemination. As such, a data provider is obliged to give priority to complying with requests for the dissemination of data from the German government, “*in the event of the casus foederis [defensive alliance] in accordance with Article 5 of the North Atlantic Treaty [ . . . ], in case of defence [ . . . ], if the requirements for the internal state of emergency [ . . . ] are satisfied, in the event of tension [ . . . ] or if there is a current danger to military or civil forces of [Germany] deployed in a foreign country or to employees of the diplomatic service [ . . . ]*” (§ 21 SDSA). While these grounds are more specific than the grounds for restricting access to remote data, they may also appear slightly broader. However, this should not concern us when considering the conformity of the SDSA with the RS Principles, as the security interests listed may not be invoked as justification for limiting the dissemination of remote sensing data, but rather require the data provider to provide such data on a priority basis (see also § 22 SDSA).

---

## Regional Level

### Introduction

The Satellite Data Security Act proved a useful example of the regulation of the dissemination of remote sensing data at the national level, for the comprehensive manner in which it approaches this issue. The Act was also highlighted because it was adopted by a State whose regulations are deeply entwined with those of a key regional player in space, the European Union. The EU manages Copernicus – formerly known as GMES (Global Monitoring for Environment and Security) – a pioneering Earth observation program for both environmental and security purposes, implemented in close partnership with the EU Member States and the European Space Agency. The Copernicus remote sensing space system has a uniquely dual composition, comprised, on the one hand, of dedicated satellites developed by the European Space Agency named Sentinels, and so-called contributing mission satellites provided by the Member States and third parties, on the other (see the Copernicus contributing missions overview page at <https://spacedata.copernicus.eu/web/cscda/missions>).

As an EU Member State with advanced national remote sensing programs, Germany contributes to Copernicus through its TerraSAR-X satellite and its “twin” TanDEM-X, as well as the RapidEye 5-satellite constellation. (See the Copernicus page for TerraSAR-X at <https://spacedata.copernicus.eu/web/cscda/missions/terrasar-x>. The satellite has been registered by Germany in the UN Space Objects Register: UN Doc. ST/SG/SER.E/526 of 29 February 2008; See the Copernicus page for TanDEM-X at <https://spacedata.copernicus.eu/web/cscda/>

[missions/tandem-x](#). The satellite has been registered by Germany in the UN Space Objects Register: UN Doc. ST/SG/SER.E/608 of 30 November 2010; See the Copernicus page for the RapidEye mission at <https://spacedata.copernicus.eu/web/cscda/missions/rapideye>. The five satellites of the constellation have all been registered by Germany in the UN Space Objects Register: UN Doc. ST/SG/SER.E/569 of 16 July 2009.) The dissemination of data from these satellites is hence subjected, in theory, to a dual national and regional legal regime. (The data disseminated by these satellites will only be subject to the Satellite Data Security Act if it is handled, as noted, “*by German nationals or by legal persons or associations of persons under German law, b) by foreign legal persons or foreign associations of persons with their head office within the territory of [Germany], or c) where the data are disseminated from within the territory of [Germany]*” (§ 1, (2) SDSA). TerraSAR-X and TanDEM-X were both financed and implemented as a public-private partnership between DLR German Aerospace Center and Airbus Defence and Space. See the page for these satellites at the DLR website at [https://www.dlr.de/dlr/en/desktopdefault.aspx/tabid-10378/566\\_read-426/#!/gallery/345](https://www.dlr.de/dlr/en/desktopdefault.aspx/tabid-10378/566_read-426/#!/gallery/345). The German branch Airbus DS Geo GmbH holds the exclusive commercial exploitation rights for both TerraSAR-X and TanDEM-X, while “*DLR is responsible for providing [...] data to the scientific community, mission planning and implementation, radar operation and calibration, control of the two satellites*” (ibid.). As for RapidEye, however, the issue is less straightforward. While the constellation of five satellites was registered by Germany and initially owned and operated by the German company RapidEye AG, ownership and operation of the constellation was later transferred following the acquisition of RapidEye AG to Canadian company BlackBridge in 2011 (prompting a name change from RapidEye AG to BlackBridge in 2013), and subsequently to US Planet Labs in 2015. As Planet Labs has its head office in San Francisco, the continued application of the SDSA depends on whether the data collected by the RapidEye satellites is disseminated from within German territory. Despite the transfer in ownership of the constellation, the RapidEye ground segment and spacecraft control centre remain located in Berlin, though the S-band and X-band downlink stations are located in Svalbard, Norway. See the information on the RapidEye constellation at the Earth Observation Portal Directory at <https://directory.eoportal.org/web/eoportal/satellite-missions/r/rapideye>. Hence, it would appear that the SDSA continues to apply to the dissemination of the data generated by the RapidEye constellation.) It was noted, however, that the German Satellite Data Security Act may not be applied to the operation of high-grade Earth remote sensing systems that are permitted under the applicable law of another Member State of the EU. Presumably this should include programs such as Copernicus that are owned and managed by the EU, and implemented by the Member States, at least as far as the contributing missions of other Member States are concerned. Yet the SDSA will only be set aside if the applicable rules contain comparable provisions and protected interests, which requires taking a closer look at the applicable Copernicus regulations. As we will see, these regulations clearly distinguish, in the elaboration of their data policy, between dedicated and contributing mission data, thus minimizing the potential for overlap between the national and regional regulatory level.

## Copernicus Regulations: Scope

The basic instruments governing Copernicus data and information are Regulation 377/2014 establishing the Copernicus Programme (Regulation (EU) No 377/2014 of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010, *OJ L* 122/44 of 24 April 2014) and Regulation 1159/2013 defining, inter alia, criteria for restricting access to such data and information. As is clear from the program's original name – Global Monitoring for Environment and Security – the scope of the remote sensing activities included in Regulation 377/2014 is wider than that of the UN Remote Sensing Principles. The Copernicus service component consists of services related to atmosphere monitoring, marine environment monitoring, land monitoring, climate change, emergency management, and, finally, the security service (Art. 5 (1) Regulation 377/2014). The objective of the Copernicus security component is “*to provide information in support of the civil security challenges of Europe improving crisis prevention, preparedness and response capacities, in particular for border and maritime surveillance, but also support for the Union's external action, without prejudice to cooperation arrangements which may be concluded between the Commission and various Common Foreign and Security Policy bodies, in particular the European Union Satellite Centre*” (Sub (f) of Art. 5 (1) Regulation 377/2014). While it is clear that this service does not, as such, fall under the scope of the RS Principles, the dual-use nature of Copernicus makes it difficult to carve the security component entirely out of the general regulations governing the program. This is clear from the definitions of the terms “Copernicus data” and “Copernicus information” – a distinction reflecting the RS Principles but not found in the SDSA – which do not differentiate between data and information collected for security or other services. (Art. 3, (7) and (8) Regulation 377/2014: “*Copernicus data*’ means dedicated mission data, contributing mission data and in situ data; ‘*Copernicus information*’ means information from the Copernicus services referred to in Article 5(1) following processing or modelling of Copernicus data [ . . . ]”)

## Open Access Policy and Security Restrictions

The EU regulation of Copernicus data and information is strongly rooted in the general open data policy developed by the Union in a string of instruments. As such, Regulation 1159/2013 notes that GMES (Copernicus) data and information should “*strongly contribute to*” ((2) of the preamble of Regulation 1159/2013) the open data policy promoted by the EU in the 2003 Directive on the Re-use of Public Sector Information (Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003, *OJ L* 345/90 of 31 December 2003), the 2010 Commission Communication “A Digital Agenda for Europe” (Commission Communication COM(2010) 245 final/2 of 26 August 2010. See also preambular paragraph (9) of Regulation 377/2014: “*Copernicus data and Copernicus information should be available freely and openly to support the Digital Agenda for Europe, as referred*

to in the Commission Communication of 26 August 2010 entitled: *A Digital Agenda for Europe.*”), and the 2011 Commission Decision on the Reuse of Commission Documents. (Commission Decision 2011/833/EU on the Reuse of Commission Documents of 12 December 2011, *OJ L* 330/39 of 14 December 2011.) Though the application of these EU policy documents is confirmed for all Copernicus data and information, Regulation 1159/2013 only applies to “GMES dedicated data” and “GMES service information,” while the relevant provisions of Regulation 377/2014 on data policy likewise single out “dedicated mission data” and “Copernicus information” (Art. 23 Regulation 377/2014). Dedicated mission data refers to “*spaceborne Earth observation data from dedicated missions for use in Copernicus*” (Art. 3, (7) Regulation 377/2014. Compare the definition for “GMES dedicated data” in Regulation 1159/2013 as referring to “*data collected through the GMES dedicated infrastructure and their metadata*” (Art. 2 (c)).), thus contrasting it with contributing mission data such as data generated by the German TerraSAR-X and TanDEM-X missions. However, the open access policy does extend to all “Copernicus information,” which should be understood as all “*information from the Copernicus services referred to in Article 5 (1) following processing or modelling of Copernicus data*” (Art. 3, (8) Regulation 377/2014. See also Art. 2, (a) and (b) Regulation 1159/2013). The latter term in turn refers to a combination of “*dedicated mission data, contributing mission data and in situ data.*” (Art. 3, (7) Regulation 377/2014. “In situ data” means “*observation data from ground-, sea- or air-borne sensors as well as reference and ancillary data licensed or provided for use in Copernicus*” (Art. 3, (5) Regulation 377/2014).) Thus, while the access policy and possible restrictions thereto elaborated in Regulations 1159/2013 and 377/2014 will apply to all information produced on the basis of all Copernicus data, the availability of the data from contributing missions that may be used as the basis for such information is still subject to the respective national regulations.

The basic rule governing access to dedicated data and information of Copernicus is laid down in Article 23, (2) of Regulation 377/2014. According to this provision, “[d]edicated mission data and Copernicus information shall be made available through Copernicus dissemination platforms, under pre-defined technical conditions, on a full, open and free-of-charge basis.” However, such full and open access is subject to a number of predefined restrictions, including the “*security interests and external relations of the Union or its Member States*” (Art. 23, (2), (c) Regulation 377/2014). The precise nature and application of this restriction is elaborated in Regulation 1159/2013. After confirming that the open dissemination principle applies to all users of “GMES dedicated data” and “GMES service information,” and noting that such data and information “*may be used worldwide without limitations in time*” (Arts. 3 and 7, (2) Regulation 1159/2013), Articles 11 and 16 of this Regulation cover a limited number of grounds on which the access to this data and information may be restricted.

According to Article 12 of Regulation 1159/2013, the Commission “*shall restrict [the] dissemination [of dedicated mission data and Copernicus information]*” only when their open dissemination “*presents an unacceptable risk to the security interests of the Union or its Member States due to the sensitivity of the data and*

*information.*” This sensitivity must be assessed by the Commission according to a predefined set of criteria. Like the Satellite Data Security Act, these criteria combine technical characteristics of the data and the time between the acquisition and dissemination with the existence of closely circumscribed situations affecting national and international security (Arts. 13 and 14 Regulation 1159/2013). These situations specifically refer to “*the existence of armed conflicts, threats to international or regional peace and security, or to critical infrastructures [, and] the existence of security vulnerabilities or the likely use of [dedicated mission data or Copernicus information] for tactical or operational activities harming the security interests of the Union, its Member States or international partners*” (Sub (c) and (d) of Arts. 13 and 14 Regulation 1159/2013). The explicit reference to international peace and security, and the inclusion of qualifiers such as “critical” when describing the security interests make clear that the Regulation is in line with the legitimate rights and interest of States that may limit the open dissemination of Copernicus data and information under international law. (The assessment of the security implications is made, inter alia, against the backdrop of the rules on EU classified information. According to Art. 25, (5) of Regulation 377/2014, “[w]here EU classified information is generated or handled within Copernicus, all participants shall ensure a degree of protection equivalent to that provided by the rules set out in the Annex to Decision 2001/844/EC and in the Annexes to Decision 2013/488/EU.” The latter documents define “EU classified information” – which, as a legal term of art, should be distinguished from the technical term “information” in the Copernicus regulations – as “any information or material designated by a EU security classification, the unauthorised disclosure of which could cause varying degrees of prejudice to the interests of the European Union or of one or more of the Member States” (Art. 2 (1) of Council Decision 2013/488/EU of 23 September 2013 on the Security Rules for Protecting EU Classified Information, OJ L 274/1 of 15 October 2013.)

Unlike the SDSA, which does not distinguish between data and information, Regulation 1159/2013 differentiates between dedicated data collected by the Sentinels and Copernicus information for the purposes of the sensitivity check. While the sensitivity check is always mandatory for Copernicus *information*, the *dedicated data* will only be subject to such test if produced by a space-based observation system capable of generating data of particularly high resolution, as defined in a separate annex to the Regulation. (Art. 13, (1) Regulation 1159/2013. The Regulation’s annex on “Characteristics of Space-based Observation System as Referred to in Article 13” defines these systems as being technically capable of generating data of geometric resolution of 2.5 m or less in at least one horizontal direction, of 5 m or less in at least one horizontal direction in the 8–12  $\mu$  spectral range (thermal infrared), of 3 m or less in at least one horizontal direction in the spectral range from 1 mm to 1 m (microwave), and of 10 m or less in at least one horizontal direction in at least one spectral channel.) And it is only where dedicated mission data are produced by a space-based observation system which does not meet *any* of the characteristics listed in the Annex, that they shall be presumed not to be sensitive (Art. 14, (2) Regulation 1159/2013). This distinction makes sense, for the sensitivity of remote sensing *information*, is not directly proportionate to the

resolution of the remote sensing observation system, unlike raw satellite data before processing and interpretation.

The sensitivity check is performed by the Commission, though it must take into account the national interests of the Member States of the EU in doing so. The preamble of Regulation 1159/2013 adds in this regard that restrictions to the open dissemination of dedicated mission data and Copernicus information “*should respect the obligations of Member States that have adhered to a common defence organisation under international treaties*” (PP (13) Regulation 1159/2013). This provision calls to mind the requirement in the SDSA for the authorities to take into account the obligations of Germany under the North Atlantic Treaty when performing the sensitivity check. Despite this integration of the concerns of Member States, the outcome of the sensitivity check may not be challenged by them, unless the conditions under which the assessment were made have changed. Only in that case may the Commission reassess the situation, either at its own initiative or at the request of Member States with a view to restricting, suspending or allowing the acquisition of dedicated mission data or the dissemination of Copernicus information (Art. 15 Regulation 1159/2013). Nevertheless, the Member States retain a final form of control through the Council, which, despite the overall responsibility of the Commission for the Copernicus security framework, “*shall adopt the measures to be taken whenever the security of the Union or its Member States could be affected by data and information provided by Copernicus.*” (Art. 25, (4) Regulation 377/2014. See also preambular paragraph (40) of Regulation 377/2014: “*As some Copernicus data and Copernicus information, including high-resolution images, may have an impact on the security of the Union or its Member States, in duly justified cases, the Council should be empowered to adopt the measures in order to deal with risks and threats to the security of the Union or its Member States.*”)

In addition to national interests of the Member States, the Commission must also take into consideration the interests of the Copernicus users and the importance of the program for the broader society. As such, Regulation 159/2013 requires that “*security interests shall be balanced against the interests of users and the environmental, societal and economic benefits of the collection, production and open dissemination of the data and information in question.*” (Art. 16 (1) Regulation 1159/2013. (2) of the same Article requires the Commission to also consider, when making its security assessment, “*whether restrictions will be effective if similar data are in any event available from other sources.*” Similar considerations must inform the outcome of the test under the SDSA.) Such general concern for the overall situation provides for a more comprehensive assessment under EU law than is the case for most national remote sensing regulations. The broader concern than mere security considerations in Regulation 1159/2013 is also apparent from the fact that access to dedicated data and Copernicus information must also be restricted when their open dissemination would conflict with other rights, including when such dissemination would “*affect in a disproportionate manner the rights and principle recognised in the Charter of fundamental Rights of the EU, such as the right for private life or the protection of personal data*” (Art. 11 Regulation 1159/2013).

## Sentinel Data

While all Copernicus information is subject to the same rules governing their open dissemination and possible restrictions, the data generated by the satellites in the Copernicus constellation will be subject to a different regime depending on whether they are acquired by Sentinels or contributing missions, or provided by third parties. As noted, Regulations 1159/2013 and 377/2014 apply only to dedicated mission data. In addition, the data generated by the ESA-developed Sentinels are also covered by a separate Sentinel data policy set jointly by the EU and ESA in 2013. (Preamble paragraph (38) of Regulation 377/2014 provides that “[t]he access rights to Copernicus Sentinel data granted under the GMES Space Component Programme as approved by the ESA Programme Board on Earth Observation on 24 September 2013 should be taken into account.”) This policy is in turn based on the Joint Principles for a Sentinel Data Policy developed by ESA and the GMES Bureau in 2009 (ESA/PB-EO(2009)98, rev. 1 of 23 October 2009). Pursuant to these Joint Principles, the Sentinel Data Policy may not distinguish between access for public, commercial, or scientific users, or between European or non-European users; the licenses for the Sentinel data shall be free of charge; and the Sentinel data will be made available online, free of charge, subject only to a generic registration process (“Joint Principles for a Sentinel Data Policy,” Annex to ESA/PB-EO(2009)98, rev. 1 of 23 October 2009, 1). The Joint Principles do foresee possible security restrictions that may affect data availability or timeliness, but limit their reach by requiring that they only be implemented for “*specific Sentinel data*,” and result in the activation of “*specific operational procedures*” (ibid., 1–2).

Following the adoption of the Joint Principles, the European Space Agency consolidated its data policy provisions for its various remote sensing missions (ERS or European Remote Sensing, Envisat and Earth Explorer) in a single document, and adapted its existing Earth Observation Data Policies to the content of the Joint Principles (see European Space Agency, “ESA Data Policy for ERS, Envisat and Earth Explorer missions,” October 2012, at [https://earth.esa.int/c/document\\_library/get\\_file?folderId=296006&name=DLFE-3602.pdf](https://earth.esa.int/c/document_library/get_file?folderId=296006&name=DLFE-3602.pdf)). The consolidated ESA policy is based on the principle that, though ownership of data provided by the ERS, Envisat, and Earth Explorer missions remains with ESA, all these data “*shall be available in an open and non-discriminatory way*” (ibid., 1). To be sure, this principle of free and open access is subject to some restrictions, as the policy distinguishes between free datasets and restrained datasets. However, the restrictions to the latter are explicitly “*due to technical constraints*” only, and are justified by the fact that “*data are not systematically processed and made available on-line*” (ibid., 2). In light of the technical reasons for these restrictions, access requests to restrained datasets are reviewed based on factors of relevance and feasibility rather than considerations of national security. Data from restricted datasets remains free of charge, unless the request concerns very large datasets, in which case a contribution may be asked.

The applicable EU and ESA documents demonstrate a clear consistency of both regional organizations’ remote sensing data policies with the UN Remote Sensing

Principles. ESA explicitly declared as much, by noting that the “*distribution of [data provided by the ERS, Envisat and Earth Explorer missions] shall be consistent with the United Nations Resolution A/RES/41/65 dated 3 December 1986 on Principles relating to Remote Sensing of the Earth from Space*” (ibid., 1). In defining the scope of application of its policy, ESA also stipulated that it applies to “*all primary and processed data (up to level 2) as defined according to the UN terminology (UN resolution 41/65)*.” This is also in keeping with the Joint Principles elaborated with the EU, which state that the UN Resolution on Remote Sensing should be taken into account as one of “*the instruments and documents [that] provide the legal and programmatic framework for the Sentinel Data Policy*” (Joint Principles for a Sentinel Data Policy, 2). Specifically, the EU-ESA Copernicus programme is also clearly in line with Principle VI of the UN Resolution, which recommends that States provide for the establishment and operation of data collecting and storage stations, and processing and interpretation facilities for remote sensing data, “*in particular within the framework of regional agreements or arrangements whenever feasible*.” (See also preambular paragraph 6 of Regulation 377/2014 (“*To promote and facilitate the use of Earth observation technologies both by local authorities and by small and medium-sized enterprises (SMEs), dedicated networks for Copernicus data distribution, including national and regional bodies, should be promoted*”).)

## Contributing Mission Data

As noted, Regulation 377/2014 makes a terminological distinction between dedicated mission data and contributing mission data, and subsequently applies its provisions on data security policy to the former only. Likewise, Regulation 1159/2013, as per its title, only defines the criteria for restricting access to “GMES dedicated data and GMES service information.” It follows that different rules may govern the access to and distribution of contributing mission data, compared to Sentinel data. The same terminological distinction is retained in Commission Implementing Decision 2018/621 on the technical specifications for the Copernicus space component. (Commission Implementing Decision (EU) 2018/621 of 20 April 2018 on the Technical Specifications for the Copernicus Space Component pursuant to Regulation (EU) No 377/2014 of the European Parliament and of the Council, *IJL* 102/56 of 23 April 2018.) This Decision, which defines the Copernicus space component as including data dissemination, and in particular the provision, archiving, and dissemination of contributing mission data (see Sections 1 and 2.1 of the Annex to the Decision), distinguishes between Dedicated Copernicus Missions (Sentinels) data and data from Copernicus Contributing Missions (CCMs) (Annex Sections 3 and 4, respectively). While the Decision confirms the open access policy for the former, it notes that “[l]icensing conditions for data shall be negotiated with contributing mission data providers for data that needs to be procured. These licensing conditions could depart from the open data policy.” (Annex Section 2.5, (a): “users have a free, full and open access to Copernicus Sentinel Data and Service Information without any express or implied warranty, including as regards quality



*and suitability for any purpose*”; Annex Section 4.3. Section 4.1 also provides that “[d]ata from CCMs could be either free of charge or could be procured under specific licensing conditions.”) To what extent the legal regulation for access to contributing missions data differs from the general EU data policy will hence depend, in practice, on the licensing terms agreed with the providers of such CCM data. These terms will depend, in part, on the municipal rules under which the data provider is operating its remote sensing activities, and may hence impose stricter limitations for reasons of national security.

Conscious of the dependency of Copernicus on the contributing missions of Member States, the Commission has committed itself to cooperating with Member States “*in order to improve the exchange of data and information between them [ . . . ] to ensure that the required data and information are available to Copernicus.*” (Art. 13 Regulation 377/2014. The provision adds that “[t]he Member States’ contributing missions, service and in situ infrastructures are essential contributions to Copernicus.” Still, CCMs are officially intended only as a complementary part of Copernicus, in that “[d]ata from CCMs shall be obtained by Copernicus to fulfil the data requirements [ . . . ], whenever these cannot be met by the Sentinels” (Section 4.1 of Decision 2018/621).) This is an application of the fundamental principle of sincere cooperation enshrined in Article 4, (3) of the Treaty on European Union (TEU), pursuant to which the Union and its Member States shall, “*in full mutual respect,*” assist each other in carrying out tasks that flow from the EU Treaties. In theory, the mutuality criterion underlying this principle also limits the discretion of Member States to restrict the remote sensing data flow under Copernicus when a more open dissemination would be considered necessary to allow the EU to perform its tasks. However, it is also an accepted principle of EU law that “[t]he provisions of the Treaties shall not preclude the application of the [rule that] no Member State shall be obliged to supply information the disclosure of which it considers contrary to the essential interests of its security.” (Art. 346 (1) of the Treaty on the Functioning of the European Union (TFEU). To the extent that national restrictions on the free dissemination of remote sensing data would be considered as limiting the free traffic between EU Member States, Art. 36 TFEU stipulates that the general prohibitions on quantitative restrictions “*shall not preclude prohibitions or restrictions on imports, exports or goods in transit justified on grounds of public morality, public policy or public security.*” See also Achilleas 2008, 9.) This follows from the fundamental notion that national security remains the sole responsibility of each EU Member State. (Art. 4, (2) TEU (“*The Union shall respect the equality of Member States before the Treaties as well as their national identities, inherent in their fundamental structures, political and constitutional, inclusive of regional and local self-government. It shall respect their essential State functions, including ensuring the territorial integrity of the State, maintaining law and order and safeguarding national security. In particular, national security remains the sole responsibility of each Member State*”).) For this reason, the Copernicus regulations explicitly note that the means of disseminating all Copernicus data and information – including dedicated mission data – and the criteria and procedures for restricting access thereto may only be regulated by the Commission “*respecting third party*

*data and information policies and without prejudice to rules and procedures applicable to space and in situ infrastructure under national control or under control of international organisations”* (Art. 24 (1) (a) and (c) Regulation 377/2014).

As illustrated by the German Satellite Data Security Act, such national laws may well require that restrictions to the dissemination of data should take into account existing obligations of the State under EU law. However, the explicit deference of both the founding treaties of the EU and the specific Copernicus regulations to the national security of Member States means that Member States will retain a large measure of discretion to withhold remote sensing data that it considers detrimental to its own interest. This does not mean, however, that the same data, or comparable data with similar security implications, could not be acquired by dedicated Copernicus Sentinels. To be sure, like all acts of the EU, the provision of Copernicus services must take into account the general principles of subsidiarity and proportionality (Art. 5 TEU). Regulation 377/2014 therefore provides that “[p]rourement of new data that duplicate existing sources shall be avoided, unless the use of existing or upgradable data sets is not technically feasible, cost-effective or possible in a timely manner” (Art. 5, (2) of the Regulation). Theoretically, however, information withheld by contributing mission partners, for reasons of national security or other, fall under this category, since their use is not “possible in a timely manner.” If the Copernicus Sentinels may hence still conceivably acquire these data – and the sweeping nature of remote sensing satellites may well make this unavoidable – their dissemination remains subjected to the general sensitivity check of Copernicus dedicated data.

---

## Conclusion

This chapter reviewed a selection of key instruments adopted to regulate the dissemination of Earth data collected by remote sensing satellites at the international, national, and regional levels. While these instruments naturally differ in terms of regulatory focus, they demonstrate sufficiently broad similarities in scope, concepts, and substantive rules so as to reveal a shared approach to the regulation of remote sensing activities.

At the international level, the 1986 UN Remote Sensing Principles focus on the freedom of States and their private actors to collect, store, and distribute remote sensing data and information, without explicit exceptions for reasons of national security. This is perhaps understandable, considering their elaboration by the Committee on the Peaceful Uses of Outer Space as a means to clarify the application of the Outer Space Treaty, whose key principles serve to safeguard the freedom of States to explore and use outer space. However, the Principles’ integration of the legitimate rights and interests of other States, as well as a general concern for international peace and security, reveals a broader context of international law that allows for an implied exception of national security to the free dissemination of remote sensing data.

This implication is rendered explicit at the national level, as illustrated, in this chapter, by the German Satellite Data Security Act of 2007. Though the Act focuses on restrictions to the free dissemination of remote sensing data, the careful formulation of these limitations indirectly confirms the free access thereto as their underlying principle. The SDSA also confirms the importance of regional integration and alliances as an important factor restricting limitations to free remote sensing data dissemination, rooted in concerns for international peace and security. In turn, the regional regulation of remote sensing, as analyzed through the lens of the rules and policies of the Copernicus programme, confirm the fundamental principle of open access to remote sensing data, while incorporating the security concerns of individual Member States of the EU. As such, instruments at both the national and regional levels not only confirm the abiding importance of the nonbinding UN Remote Sensing Principles but also clarify their application by means of a detailed set of rules and policies that aim to strike a balance between public security and public access to information in a free market.

---

## References

### International Instruments

#### Treaties

- African Charter on Human Rights and Peoples' Rights of 27 June 1981, 1520 *UNTS* 217  
 American Convention on Human Rights of 22 November 1969, 1141 *UNTS* 123  
 Chicago Convention on International Civil Aviation of 7 December 1944, 15 *UNTS* 295  
 Constitution and Convention of the International Telecommunication Union (2018 version), published in the Basic Texts of the ITU, 2019  
 Convention for the Protection of Human Rights and Fundamental Freedoms of 4 November 1950, 213 *UNTS* 222  
 Convention on the Transfer and Use of Data of Remote Sensing of the Earth from Outer Space of 19 May 1978, annexed to UN. Doc. A/33/162 of 29 June 1978  
 International Covenant on Civil and Political Rights of 16 December 1966, 999 *UNTS* 171  
 Paris Convention relating to the Regulation of Aerial Navigation of 13 October 1919, *Br. Treaty Series* 1923, No. 14  
 Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies of 27 January 1967, 610 *UNTS* 8843

#### UNGA Resolutions

- Concerted Action for Economic Development of Economically Less Developed Countries, UN Doc. A/RES/1515 (XV) of 15 December 1960  
 Permanent Sovereignty over Natural Resources, UN Doc. A/RES/1803 (XVII) of 14 December 1962

- Principles Relating to Remote Sensing of the Earth from Outer Space, UN Doc. A/RES/41/65 of 3 December 1986
- Recommendations on National Legislation relevant to the Peaceful Exploration and Use of Outer Space, UN Doc. A/RES/68/74 of 11 December 2013
- Universal Declaration of Human Rights, UN Doc. A/RES/217A (III) of 10 December 1948

## UN Documents

- Answers from the Chair of the Space Law Committee of the International Law Association (ILA) to questions by the Chair of the Working Group of the LSC, UN Doc. A/AC.105/C.2/2015/CRP.25 of 22 April 2015
- Information furnished in conformity with the Convention on Registration of Objects Launched into Outer Space, UN Doc. ST/SG/SER.E/526 of 29 February 2008
- Information furnished in conformity with the Convention on Registration of Objects Launched into Outer Space, UN Doc. ST/SG/SER.E/569 of 16 July 2009
- Information furnished in conformity with the Convention on Registration of Objects Launched into Outer Space, UN Doc. ST/SG/SER.E/608 of 30 November 2010
- Report of the Legal Sub-Committee on the Work of its Eleventh Session (10 April–5 May 1972), UN Doc. A/AC.105.101 of 11 May 1972

## European Instruments

- Commission Communication COM(2010) 245 final/2 of 26 August 2010
- Commission Decision 2011/833/EU on the Reuse of Commission Documents of 12 December 2011, *OJ L* 330/39 of 14 December 2011
- Commission Delegated Regulation (EU) No. 1159/2013 of 12 July 2013 supplementing Regulation (EU) No. 911/2010 of the European Parliament and of the Council on the European Earth monitoring programme (GMES) by establishing registration and licensing conditions for GMES users and defining criteria for restricting access to GMES dedicated data and GMES service information, *OJ L* 309/1 of 19 November 2013
- Commission Implementing Decision (EU) 2018/621 of 20 April 2018 on the Technical Specifications for the Copernicus Space Component pursuant to Regulation (EU) No 377/2014 of the European Parliament and of the Council, *IJ L* 102/56 of 23 April 2018
- Council Decision 2013/488/EU of 23 September 2013 on the Security Rules for Protecting EU Classified Information, *OJ L* 274/1 of 15 October 2013
- Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003, *OJ L* 345/90 of 31 December 2003
- European Space Agency. ESA Data Policy for ERS, Envisat and Earth Explorer missions, October 2012. [https://earth.esa.int/c/document\\_library/get\\_file?folderId=296006&name=DLFE-3602.pdf](https://earth.esa.int/c/document_library/get_file?folderId=296006&name=DLFE-3602.pdf). Accessed 18 Apr 2019
- Joint Principles for a Sentinel Data Policy, ESA/PB-EO(2009)98, rev. 1 of 23 October 2009
- Regulation (EU) No 377/2014 of the European Parliament and of the Council of 3 April 2014 establishing the Copernicus Programme and repealing Regulation (EU) No 911/2010, *OJ L* 122/44 of 24 April 2014

## National Instruments

- Canada, Act Governing the Operation of Remote Sensing Space Systems, Bill C-25 of 25 November 2005
- France, Loi Relative aux Opérations Spatiales, N° 2008518, 3 June 2008, as most recently amended on 30 May 2013. <https://www.legifrance.gouv.fr/affichTexte.do?cidTexte=LEGITEX T000018939303>
- Germany, Act to give Protection against the Security Risk to the Federal Republic of Germany by the Dissemination of High-Grade Earth Remote Sensing Data of 23 November 2007, 2590 *Federal Gazette (BGBl.)*, Year 2007, Part I, No. 58, 28 November 2007
- India, Remote Sensing Data Policy of 2011, RSDP-01:2001. [https://nrsc.gov.in/Remote\\_Sensing\\_Data\\_Policy](https://nrsc.gov.in/Remote_Sensing_Data_Policy). Accessed 18 Apr 2019
- Japan, Act on Securing Proper Handling of Satellite Remote Sensing Records, Act No. 77 of 2016. Available with English translation via [https://www8.cao.go.jp/space/english/rs/rs\\_act.pdf](https://www8.cao.go.jp/space/english/rs/rs_act.pdf). Accessed 18 Apr 2019
- Japan, Basic Space Law, Act No. 43 of 28 May 2008, with unofficial English translation in *J Space L* 34(2008):471
- United States, 51 US Code Subchapter III – Licensing of Private Remote Sensing Space Systems, § 60122

## Doctrine

- Achilleas P (2001) High-resolution remote sensing imagery and human rights. *Proc Colloq Law Outer Space* 44:234
- Achilleas P (2008) French remote sensing law. *J Space Law* 34:1–9
- Aoki S (2010) Japanese law and regulations concerning remote sensing activities. *J Space Law* 36:335–364
- Bosc PA (2015) Earth observation for security and dual-use. In: Schrogl K-U et al (eds) *Handbook of space security: policies, applications and programs*. Springer, New York
- Cheng B (1997) *Studies in international space law*. Clarendon, Oxford
- De Beer AC (2015) The refusal of access to high resolution remote sensing data for reasons of national security: a (new) rule of customary international law? [https://repository.up.ac.za/bitstream/handle/2263/53120/DeBeer\\_Refusal\\_2016.pdf;sequence=1](https://repository.up.ac.za/bitstream/handle/2263/53120/DeBeer_Refusal_2016.pdf;sequence=1). Accessed 18 Apr 2019
- Lee RJ (2001) Military use of commercial remote sensing data. *Proc Colloq Law Outer Space* 44:248
- Lyall F, Larsen PB (2009) *Space law – a treatise*. Ashgate, Farnham
- Mantl L (2015) Principle XIV [of the RS Principles] (International responsibility). In: Hobe S, Schmidt-T B, Schrogl K-U (eds), *Cologne Commentary on Space Law*, vol 1. *Outer Space Treaty*, Carl Heymanns Verlag, Köln
- Schmidt-Tedd B, Kroymann M (2008) Current status and recent developments in German remote sensing law. *J Space Law* 34:97–140
- Smith LJ, Reynders M (2015) Historical background and context [of the RS Principles]. In: Hobe S, Schmidt-T B, Schrogl K-U (eds), *Cologne Commentary on Space Law*, vol 1. *Outer Space Treaty*, Carl Heymanns Verlag, Köln

---

## **Part IV**

# **Space Security Programs Worldwide and Space Economy Worldwide**



# Space Security Programs and Space Economy: An Introduction

# 58

Christina Giannopapa

## Contents

Introduction .....	1125
Space Security Programs .....	1126
The Economy of the Space Sector .....	1129
The Role of International Organizations for Space Security .....	1130
Conclusions .....	1131
References .....	1131

## Abstract

This chapter provides an introduction to Part 4 of the second edition of the *Handbook of Space Security* addressing the subject of “Space Security Programs Worldwide.” It covers expert views on space security activities and programs of established spacefaring nations: the United States, Russia, China, Europe – including dedicated chapters on France, Italy, the United Kingdom – and India. It also reviews space security policies of emerging space countries – Australia, Iran, and Pakistan – to showcase a wide range of space activities and programs worldwide. Additionally it covers the economy of the space sector and it provides an overview of the UN space security-related organizations.

## Introduction

Space activities in the past were only the privilege of the governments of a few space-faring nations. Over the past years there has been an increase in space activities, with the number of nations with space priorities also increasing. Space

---

C. Giannopapa (✉)  
European Space Agency (ESA), Paris, France  
e-mail: [christina.giannopapa@esa.int](mailto:christina.giannopapa@esa.int)

programs are designed around two main political arguments: access to independent information to support government interests and access to critical technologies and capabilities. The governments' space programs have traditionally been designed to respond to programmatic objectives-related launchers and satellites, and nowadays also include applications. The launchers and satellite programs, civilian or military oriented, are often developed to reflect security objectives. The dual nature of space technologies and applications makes it difficult to strictly define space security programs in isolation.

In the twentieth century, launcher programs have been closely related to classified military projects demonstrating intercontinental ballistic missile capabilities (ICBM). Over the years they have seen a gradual level out to commercial launches separated from the military activities. Many countries still consider their launch program as a priority in order to gain independent access to space. Today, besides the United States and Russia, the European Space Agency, Japan, China, India, Iran, and Israel also possess launch capabilities. Most of these countries or agencies are offering services also on a commercial basis providing through their launch vehicles access to put satellites to space to many more countries around the world (Euroconsult 2019).

On October 4, 1957, the Soviet Union's space program put in space the first artificial satellite Sputnik 1. Initial satellite programs were set to fulfill science and military objectives. Today, there are more than 50 countries in all continents that have a satellite in orbit. Almost 1,000 operational satellites are now in orbit with diverse Earth observation, telecommunications, navigation, and positioning missions. In parallel to the growing importance of these down-to-earth applications, science and space exploration remain key missions of space agencies, invigorating international scientific cooperation. The United States leads with more than 250 satellites in orbit, followed by Russia and China (Euroconsult 2019). The new landscape of space-faring nations is the result of two trends: the ambition of many countries around the world to develop independent national space programs and the globalization of the aerospace and defense industry.

This chapter of the Handbook introduces different space activities and launch/satellite programs of established spacefaring nations: the United States, Russia, China, Europe – including dedicated chapters on France, Italy, the United Kingdom – and India and also emerging space countries – Australia, Iran, and Pakistan – to showcase a wide range of space activities and programs worldwide. The section covers also the space sector economy, the political economy of outer space security, and the New Space economy consequences as indicated by the space programs worldwide. It concludes with an overview of the UN space security-related organizations, due to the influence that they may have over the development of the space programs across the world.

---

## Space Security Programs

The space programs of the *United States* (US) military and intelligence organizations constitute by far the world's largest space program. The services provided by these programs include telecommunications, surveillance, missile early warning,



meteorology, positioning/timing, radio interception, nuclear detonation detection, and data relay. ► [Chapter 59, “Satellite Programs in the USA”](#) describes how the space systems provide both tactical and strategic services to the US military and intelligence agencies and in some cases to those of its allies. Strategic functions include monitoring international security treaties, analyzing the security forces of current and potential adversaries, and providing information to the President and the Secretary of State. Tactical functions include supporting US military and intelligence forces around the world. Overall, the US military space program continues to dwarf (a) the military space programs of all other countries combined and (b) of US civilian agencies such as NASA. The United States is unique in deploying military satellites of all types and on a global basis, and there is little sign that this will change in the next decade.

*Russia* can be considered today as having the most complete launch program in the world. Russia currently operates four types of launch vehicles, the Rockot, Soyuz, Zenit, and Proton. ► [Chapter 60, “Russian Space Launch Program”](#) explains how Russia has been successfully engaged in space activities for more than 60 years, having entered the space age as part of the Soviet Union and striding on as a separate state. On the one hand, after the dissolution of the USSR, Russia inherited the huge scientific and technical potential and technological developments of one of the two most powerful space nations of that time. But on the other hand, Russia was deprived of a large part of technologies and infrastructure put in place earlier. The launch vehicles that used to be Soviet became foreign, and the key launch site turned out to be located outside Russia’s national territory. Also, it proved to be difficult for Russia to use remnants of its own technologies. For Russia, space is thus not only a question of national defense and security or its position in the market of commercial launch services but also, and more importantly, a question of the status of Russia as a highly developed nation in terms of science and technology.

In *Europe*, the 2019 Regulation for a Space Programme proposes the development of Governmental Satellite Communications (GOVSATCOM) and Space Situational Awareness (SSA) programs to accompany the satellite navigation program Galileo and the Earth observation program Copernicus. The European family of launchers includes the Ariane 5, Vega, and Soyuz that secure Europe’s independent access to space and are launched through the Guiana Space Centre. During the Ministerial Council 2019, the European Space Agency (ESA) has recently adopted a safety and security program and has also secured the transition to the next generation of launchers: Ariane 6 and Vega-C, as well as the Space Rider, ESA’s new reusable spaceship. The chapters on institutional and national space and security programs in Europe describe how the aforementioned institutional programs are intertwined with the national and multilateral programs of the European States based on their national budgets and contributions to organizations such as ESA, EU, European Defence Agency (EDA), and NATO. Overall, the space activities and programs of European States address the fields of Earth observation, satellite communication, Global Navigation Satellite System (GNSS), SSA, space transportation, satellite operations, and detection, tracking, and warning. The French, Italian, and British space programs are presented in separate chapters in greater detail.

*France* is historically the third space-faring nation. After more than 50 years of dedicated vision and investments in space industry and programs, ► [Chap. 65, “Future of French Space Security Programs”](#) explains how France has developed innovative and credible capabilities which ensure its independence and constitute a tangible asset contributing to the development of coherent European defense space cooperation. In direct connection with the new Defense Space Strategy sought by the President of the Republic, modernization of current capabilities is the challenge of the coming years for France.

*Italy* has a very long history and heritage in the space sector. ► [Chapter 66, “Italy in Space: Strategic Overview and Security Aspects”](#) describes how beginning in the 1950s, with the development of the first national satellite, the San Marco 1, and its launch, operated by an Italian team, Italy entered into a period of rapid growth for space technologies, applications, and cooperation at international level. Today, Italy is the third contributor of the European Space Agency, and it has, at national level, the knowledge and the experience in the whole chain of supply in space.

*Britain* stands at something of a crossroads in its development of spacepower, not least in its military and security elements. ► [Chapter 67, “British Spacepower: Context, Policies, and Capabilities”](#) explains how spacepower is coming of age within the United Kingdom, not least in the military dimension. The British state is at something of a crossroads when making choices about its future space development as it has to respond to turbulence across the transatlantic region.

*China’s* development of launch vehicles is sticking to the “self-reliance and independent innovation” path. ► [Chapter 69, “Chinese Space Launch Program”](#) describes how, with more than 50 years of experience, China has successfully developed more than 10 models of launch vehicles and managed the transition from research test to flight application, and from flight application to industrialization. The Long March is its primary expendable launch system family. This chapter provides an overview of China’s space launch plan. This chapter mainly presents the development history of China’s launch vehicles, launch vehicles in service, the new generation of launch vehicles under development, as well as the efforts made by China in the field of space security. In addition, ► [Chap. 68, “Chinese Satellite Program”](#) explains the development history and outlines specific satellite programs: Earth observation, communications and broadcasting, navigation and positioning, and scientific and technological test satellites. In addition, it addresses the satellite program’s future perspectives and China’s international exchanges and cooperation.

The *Indian* launch program started with the vision to utilize the potential of space technology and its applications for national development in the 1960s. ► [Chapter 70, “Indian Space Program: Evolution, Dimensions, and Initiatives”](#) describes the significant progress that India has made in launch vehicle technology. Over the years India has been developing the Satellite Launch Vehicle which retired in 1984: the Augmented Satellite Launch Vehicle; the Polar Satellite Launch Vehicle; and the Geosynchronous Launch Vehicle, and is making efforts for Reusable Launch Vehicles. One of the important missions accomplished in the recent past is the development and operationalization of the new launch vehicle, GSLV MkIII. India’s next milestone mission of Human Spaceflight has been initiated and the first crewed flight

is expected by 2022. As of September 2019, Indian Space Research Organisation (ISRO) has accomplished 184 missions, including 101 satellite missions, 73 launch vehicle missions, and 10 technology demonstration missions.

The space sector in *Australia* is experiencing an unprecedented level of public interest and government support. National security considerations and the economic benefits of a fast-growing world market for space products and services are inextricably linked as drivers for a range of government and industry initiatives, as explained in ► [Chap. 71, “Australia’s Space Security Program.”](#) The government’s clear intention is to enhance Australian Defence sovereign space capabilities progressively through access to allied and commercial space-based capabilities. Australia as a nation is exposed to and provide evidence that Australia is now treating space as an integral component of its role in the protection of its national security interests and in the advancement of its international responsibilities.

Despite political, technological, and economic constraints, *Pakistan* is considered an aspiring space power with a relatively modest space program compared to the larger, more successful ones of China and India. ► [Chapter 72, “Pakistan’s Space Activities”](#) describes how the country can utilize available resources to improve its nascent space infrastructure through collaborative efforts to gain eventual self-sufficiency for socioeconomic and strategic purposes in the South Asian region. The concept of multilateral collaboration, utilizing available resources and public-private partnerships to empower its space program, enhances its domestic scientific and technological base and builds an indigenous space industry that can reap dividends at home and abroad.

---

## The Economy of the Space Sector

The *Space Sector Economy* over the years has become more commercial, and different space applications have emerged outside the traditional research and development (R&D), calling for a wider definition of space economy. This wider “space economy” can be defined using different angles. It can be defined by its products (e.g., satellites, launchers), by its services (e.g., broadcasting, imagery/data delivering), by its programmatic objectives (e.g., military, robotic space exploration, human spaceflight, Earth observation, telecommunications), by its actors/value chains (from R&D actors to users), and by its impacts (e.g., direct and indirect benefits). ► [Chapter 73, “Space Sector Economy and Space Programs World Wide”](#) describes how the worldwide national space budgets have continued to grow in 2017 and 2018. In the area of defense space programs, funding is expected to increase until 2025. In 2018, the United States is dominating with 71.7% of the world total. In relative terms, Asian spending on military space activities has more than doubled over the period between 2008 and 2018, strongly driven by China along with significant Japanese budget allocations, and is expected to increase further from \$3.49 billion to \$5.19 billion in 2025. Europe is the fourth largest region in terms of space defense spending, totaling \$1.30 billion following the United States, Asia, and CIS countries (Russia). Ariane 6 development is approaching its final phase, which

may lead to reduced defense space contributions in Europe. The foreseen growth in space defense spending is mainly driven by the United States, China, India, and Japan (Euroconsult 2019).

These figures are justified by *New Space Economy* as a new paradigm able to revolutionize space activities. ► Chapter 74, “The New Space Economy: Consequences for Space Security in Europe” states that there is a large consensus of perceptions which tends to define this set of US-led policies and investments as a shift for all space activities. This is the reason why it is triggering effects worldwide and creating a new context for European space activities. In Europe, space policies have often been characterized by a dialectic between plurality and collaborative common frameworks. The fragmented European space landscape has always found it difficult to respond to the critical mass developed by US public and private policies. This is today the case with the “new space economy,” where the United States is fundamentally renewing its public policy in order to create a more efficient and business-friendly approach to space, a shift which has helped create a new breed of space entrepreneurs, IT tycoons investing in space with considerable financial capabilities, and tech incubator methodologies. This paradigm has renewed investments, technologies, and a new spirit of space conquest and puts enormous pressure on the European space sector, which has to renew its classic approach. Europe needs to come up with a more strategic space vision that is able to take into account not only the outcomes of new technology but also the inbred characteristics of space-based technology production and data fluxes, with key issues in terms of security.

As human civilizations increasingly explore, utilize, and compete in space, the man-made security challenges are evolving and the strategies and *Political Economic* rationales become increasingly relevant for analysis. As such, ► Chap. 75, “Political Economy of Outer Space Security,” sustainability and efficiency call for exploitation of static economies of scale and scope in space industries and services, yet the trade-offs in control, governance, and dynamic innovation point toward autonomy and oligopolistic structures with overcapacity. The economic sustainability becomes a key element of the dynamic pursue of space policies and objectives at national and partnership levels. In the latter case, specialization and its implications for the wide economy through externalities and indirect effects receive increasing attention as space becomes contested, congested, and competitive. Notwithstanding the fact that they are largely government controlled, aerospace industries play a crucial role in trading patterns. Hence, they can be considered a fiscal government spending element similar to defense expenditure. The country specializations and their evolution in commercial markets and alliances are focal points in the current global trade policy paradigm shifts, affecting performance

---

## The Role of International Organizations for Space Security

The various initiatives being discussed in the different UN *fora* indicate the increasing pressures facing the international community in addressing all aspects of space security and strengthening the multilateral regime governing the use of space.

However, they also reveal substantial differences among states over priorities, methodologies, mechanisms, and programmatic settings to address and tackle space security issues. ► [Chapter 76, “Views on Space Security in the United Nations”](#) describes how this proliferation of initiatives which offers distinct approaches that look at both short- and long-term solutions might pose more challenges to the existing discussions. More worrisome, however, may be another challenge: deadlocks in the work of one body can be transferred over other fora, limiting progress even on those aspects on which there has traditionally been consensus. Existing frictions among different UN bodies are also a limiting factor in pushing forward a shared agenda on space security, and so too is the long-standing division between civilian and military uses of space embedded in the UN machinery. While divergent perceptions and priorities among leading space powers still exist (and will remain), the existence of political will that accommodates, rather than eliminates, these differences can prove effective in finding common ground for future action that can be acceptable for the interests of different states. As the nature of risks to space infrastructure and services, and the available responses, are similar (although not entirely) for all space actors – whether civilian, commercial, or military – common threat perceptions may influence how states choose to cooperate and readily serve as a basis for developing common responses and finding future consensus.

---

## Conclusions

Space programs aiming at the development and utilization of space technologies and applications constitute an essential part of capabilities in the security domain related to both civil and defense. The dual nature of space technologies and applications makes it difficult to strictly define space security programs in isolation. As the number of countries involved in space activities is increasing, there is an increasing need for ensuring both space for security and security in space.

---

## References

Euroconsult (2019) Government space programs. Benchmarks, Profiles & Forecasts to 2028



Pat Norris

## Contents

Introduction .....	1134
Background .....	1135
Telecoms .....	1136
Introduction .....	1136
Advanced Extremely High Frequency (AEHF) and Milstar .....	1138
MUOS and UFO .....	1140
Wideband Global SATCOM (WGS) .....	1143
Data Relay .....	1144
Interim and Enhanced Polar System (IPS/EPS) .....	1145
Global Positioning System (GPS) .....	1146
Surveillance .....	1151
Introduction .....	1151
Optical Imaging Satellites .....	1151
Imaging Radar Satellites .....	1154
Missile Early Warning Satellites .....	1155
Nuclear Detonation Detection System .....	1158
Signals Intelligence Satellites: Non-maritime .....	1159
Maritime Signals Intelligence Satellites .....	1161
Weather Satellites .....	1162
Other Satellites .....	1164
Space-Based Space Surveillance (SBSS) .....	1164
GSSAP .....	1165
Research Satellites .....	1166
Future Prospects .....	1168
Conclusions .....	1169
References .....	1169

---

P. Norris (✉)  
VAPN Ltd, West Byfleet, UK  
e-mail: [pat@vapn2.com](mailto:pat@vapn2.com)

---

**Abstract**

The space programs of the US military and intelligence organizations are described. The services provided by these programs include telecommunications, surveillance, missile early warning, meteorology, positioning/timing, radio interception, nuclear detonation detection, and data relay. Both unclassified and classified programs are described, with less detail and more speculative information for the latter. Recent trends that indicate the focus of future programs are discussed.

---

**Introduction**

In this chapter what is by far the world's largest space program is described. Up until 2011 the space budget of the Department of Defense (DOD) was reported in the media as being between \$20 billion and \$22 billion each year this century. Since then the published figure is about half that, i.e., \$10–12 billion per annum, apparently due to removal of intelligence-related space programs from the reported budget figures. For the period 2011 to 2013, figures reported in *The Washington Post* based on information leaked by Edward Snowden indicated that the National Reconnaissance Office (NRO) and the National Geospatial-Intelligence Agency (NGA) had a combined budget of \$15–16 billion per annum, which should probably be considered as part of US Government space security activities. Information about NRO and NGA funding in more recent years has not been published, but it seems likely that the full US space security budget is currently in excess of \$20 billion per annum.

The space programs of the US military and intelligence communities are treated in this chapter as being one and the same. The NRO is a joint agency of DOD and the Central Intelligence Agency (CIA) in order to deliver space systems that serve both parent organizations.

The large number of programs is broken down in this chapter as follows:

- Telecommunications (Section “[Telecoms](#)”)
- Global Positioning System (Navigation) (Section “[Global Positioning System \(GPS\)](#)”)
- Surveillance (Section “[Surveillance](#)”)
- Other (Section “[Other Satellites](#)”)

The descriptions include the ground elements for control of the relevant missions but exclude the user equipment and other stand-alone ground systems. In general, only operational systems are described, with just a few of the very large number of research, prototype, demonstration, and preoperational space systems mentioned in section “[Other Satellites](#).”

## Background

The space systems described in this chapter provide both tactical and strategic services to the US military and intelligence agencies and in some cases to those of its allies. Strategic functions include monitoring international security treaties, analyzing the security forces of current and potential adversaries, and providing information to the President and the Secretary of State. Tactical functions include supporting US military and intelligence forces around the world.

The higher cost of many US military space systems compared to commercial systems is due in part to their hardening against nuclear explosions in space, their ability to resist jamming and other forms of interference, and their ability to operate autonomously in the absence of ground control systems.

The launchers used by the DOD are not described in this chapter since they are used for civilian as well as military missions. From 2007 to 2016, United Launch Alliance (ULA), a joint venture between Boeing and Lockheed Martin, was the sole source provider of launch services to DOD and NRO for medium and heavy lift. Despite steadily rising launch costs, the company maintained its position based on the performance and reputation of its two vehicles, Atlas V and Delta IV, and the lack of viable competition. In 2016 SpaceX broke the ULA monopoly by winning a contract to launch a GPS-III satellite on its Falcon 9 rocket at a price of \$83 million, about 40% less than ULA had previously charged, according to Lt. Gen. Samuel Greaves, then head of the Air Force's Space and Missile Systems Center. As of March 2019, SpaceX has won ten Air Force launch contracts, eight for Falcon 9, and two for Falcon Heavy: the latter two are the Space Test Program-2 (STP2) demonstration mission that comprises 25 small spacecraft (2019 launch) and the Air Force Space Command (AFSPC)-52 satellite whose mission is classified (2020 launch). The price of the Falcon Heavy for the AFSPC satellite was \$130 million. The price differential between SpaceX and ULA was highlighted in February 2019 by the award of three launch contracts to each for 2021–2022 launches: \$297 million to SpaceX to launch AFSPC-44, NROL-85, and NROL-87, averaging \$99 million per launch, and \$441.76 million to ULA to launch SBIRS GEO-5, SBIRS GEO-6, and Silent Barker, a classified space situational awareness mission, averaging 48% more than SpaceX at \$147 million per launch.

In October 2018 the Air Force awarded three contracts for the development of Blue Origin's New Glenn (\$500 million), Northrop Grumman's Omega (\$792 million), and ULA's Vulcan Centaur (\$967 million) launch vehicle prototypes. In 2020 two contractors are to be selected to compete for up to 25 national security launches to be awarded from 2022 to 2027 based on a selection process beginning in 2019 (which SpaceX and any other launch supplier can enter). One of the triggers for this initiative is the Congressional ban on the use of the Russian RD-170 engine in ULA's Atlas V rocket from 2022. Some Members of Congress are questioning the fairness of the award to the three companies because of their concerns that it puts SpaceX at a competitive disadvantage for the 2020 selection.



Congress enacted \$2.1 billion for five launches in Fiscal Year (FY) 2019, and \$1.7 billion has been requested by DOD for FY2020 for four launches.

Smaller launcher options for DOD and NRO include Northrop Grumman's Minotaur and Pegasus.

The following references have been used in compiling this chapter:

- Information about unclassified programs has mainly been drawn from:
  - The DOD program fact sheets
  - The DOD AU-18 Space Primer
- Information about classified programs has mainly come from:
  - *Watching Earth from Space* by the author of this chapter and references therein, especially:  
*The US Intelligence Community* by J T Richelson

The information in these references has been updated based mainly on information in the trade press, including *Aviation Week & Space Technology*, *Air & Cosmos* (in French), and *Space News* and budgetary information reported in *The Washington Post* on August 29, 2013, based on documents leaked by Edward Snowden.

---

## Telecoms

### Introduction

80% of all communications to US deployed military forces travel through satellite. And 80% of that traffic is carried through commercial communications satellites – DOD spent over \$600 million in 2010 leasing services from commercial satellite operators. The remaining 20% of the 20% of traffic to deployed forces is carried by special purpose military communications satellites. Commercial satellites are used wherever possible so that in case of an urgent need, capacity is available on the military satellites.

The use of commercial satellites has led to some embarrassing moments for the US military. On several occasions, the transmissions from remotely controlled aircraft have been intercepted by journalists and made public. There has been no persuasive rationale offered as to why these transmissions are not encrypted other than that the remotely controlled aircraft were of a vintage that did not carry encryption facilities. Given the ubiquitous and low cost of mass market encryption/decryption technology as used, for example, in cell phones and pay-TV, many commentators have wondered why the encryption technology is supposedly too modern or expensive for remotely controlled aircraft that cost more than \$1 million each. The proliferation of remotely controlled aircraft since 2003 has called for an increasing amount of satellite communications capacity – particularly the large long-duration drones that are controlled from bases in the USA even when flying in Central Asia.

The US's specialist military communications satellites provide a mix of strategic and tactical services to forces on land, at sea, and in the air. Three parts of the radio spectrum are used for the transmissions, ultrahigh frequency (UHF, below 1 GHz), X-band (6–8 GHz), and extremely high frequency (EHF, 20–30 GHz).

Satellites currently in orbit include a mix of a new generation of systems and those of the previous generation. By 2020 it is expected that the DOD satellite communication services will be carried by 16 of the new generation systems – 4 AEHF, 8 WGS, and 4 MUOS – described in the next three sections. These 14 will be augmented by (a) EHF payloads on polar-orbiting satellites to provide Arctic coverage (Section “[Interim and Enhanced Polar System \(IPS/EPS\)](#)”), (b) data relay satellites (Section “[Data Relay](#)”), and (c) commercial satellites.

In the past each service had its own communications satellites, but with the current systems, the user doesn't necessarily know which satellite he is using. Connections are provided by the Global (or Regional) SATCOM Support Center (GSSC) based on the availability of the appropriate bandwidth in the relevant areas. As of December 2018, GSSC is part of the US Air Force Space Command. Previously, commercial satellite services had been the responsibility of a unit of the Defense Information Systems Agency (DISA). Air Force Space Command will absorb the Enhanced Mobile Satellite Services program, also known as the Iridium satellite program office, as well as DISA's commercial satellite leasing team. As of November 8, 2018, DISA had 91 active commercial SATCOM leases that are worth about \$4.5 billion, according to Clare Grason, division chief for satellite communications at DISA.

To improve the value for money of the commercial SATCOM services it purchases, the DOD is no longer insisting on lowest price technically acceptable (LPTA) selection of supplier for each purchase. The alternative Blanket Purchase Agreement (BPA) approach has been used, for example, to purchase O3b medium Earth orbit (MEO) satellite services from SES. This BPA allows military users to purchase SES O3b MEO managed services up to \$516.7 million over 5 years. By putting the BPA in place, the DoD has been able to drastically cut the amount of time needed to acquire satellite services, as well as negotiating a bulk purchase price as opposed to the high spot prices often associated with the LPTA approach.

The remainder of this section is structured as follows:

- AEHF and Milstar (Section “[Advanced Extremely High Frequency \(AEHF\) and Milstar](#)”)
- MUOS and UFO (Section “[MUOS and UFO](#)”)
- WGS (Section “[Wideband Global SATCOM \(WGS\)](#)”)
- Data Relay (Section “[Data Relay](#)”)
- Interim and Enhanced Polar System (Section “[Interim and Enhanced Polar System \(IPS/EPS\)](#)”)

## Advanced Extremely High Frequency (AEHF) and Milstar

The White House National Security Council, chaired by the President, uses the AEHF satellites (see Fig. 1) to control tactical and strategic forces on missions around the globe and at all levels of conflict. Four AEHF satellites are in geosynchronous orbit, launched in 2010, 2012, 2013, and 2018, with two more planned in 2019 and 2020. They combine (a) a strategic communications mission, i.e., assured jam-proof connectivity between the President and nuclear forces, and (b) protected tactical communications. These two quite distinct missions share equipment on the satellite such as a digital core processor. The strategic mission requires the satellites to be radiation hardened to survive a nuclear explosion in space and other threats, which critics have argued makes AEHF more expensive than two separate satellites would have been (one for the strategic mission, the other for the tactical).

Each AEHF weighs about 6½ t when launched on an Atlas 5 from Cape Kennedy and is based on the Lockheed Martin A2100 spacecraft bus (also used for commercial satellites) with a Japanese IHI BT-4 apogee thruster and an electric propulsion system. The electric ion propulsion system is intended for maneuvering the satellite in its final orbit but was called into action on AEHF-1 when the apogee thrust motor failed. The slow evolution from the elliptical transfer orbit into which the Atlas 5 placed the satellite on August 14, 2010, and the eventual geostationary orbit took 16 months using the low thrust ion engine. A further 5 months were required for on-orbit testing until AEHF-1 became operational in March 2012. Ironically, in early 2012 Boeing announced the sale to two commercial satellite operators of four “all electric” satellites, which do away entirely with chemical propulsion. These satellites will take 4 to 6 months to reach their operational orbit but are significantly lighter (and therefore cheaper) than the conventional satellites that achieve their operational orbit in days rather than months.

**Fig. 1** AEHF satellite



Credit: USAF

Artist's impression of AEHF in orbit

The space segment consists of a cross-linked constellation of two satellites with a planned extension to four, forming a ring at geosynchronous orbit that provides continuous communications without the need for a ground-hop. They provide communications at a variety of data rates from 75 bps to approximately 8 Mbps and broadly provide ten times the throughput of the 1990s-era Milstar satellites with a substantial increase in coverage for users. System uplinks and cross-links operate in the extremely high frequency (EHF) range and downlinks in the superhigh frequency (SHF) range. The communications are channeled through an antenna farm on each satellite comprising:

- Two SHF downlink phased arrays
- Two cross-link antennas
- Two uplink/downlink nulling antennas
- One uplink EHF phased array
- Six uplink/downlink gimballed dish antennas
- One each uplink/downlink Earth coverage horn

The four-satellite constellation will allow the military to deliver an extended data rate (XDR) service, which in practical terms will deliver video in hours rather than days, and allow data to be transferred in seconds rather than minutes. But the XDR capability will not likely be on offer until more of the ground and airborne terminals are available for use, in about 2020 (more than a decade after the first satellite was launched). The terminals for airborne and ground-based users that have not yet been fielded are known as the Family of Beyond Line-of-Sight Terminals (FAB-T).

In 2015, the ground/air terminal program (prime contractor Raytheon) was split into (a) command post terminals to facilitate communications for nuclear and conventional forces through the E-6 and E-4 aircraft and (b) force element terminals to provide the capability to the B-2 and B-52 bomber and the RC-135 Rivet Joint intelligence, surveillance, and reconnaissance aircraft. The Government Accountability Office has said that all six AEHF satellites are expected to be on-orbit before FAB-T is operational.

Under a contract valued at \$6.6 billion, Lockheed Martin supplied four AEHF satellites, and a further two have since been ordered to bring the total order value to about \$9 billion. Northrop Grumman is responsible for the EHF payload.

The AEHF constellation is also used by Canada (at a cost of \$592 million), the Netherlands, and the UK, while Australia, Japan, and NATO are negotiating to join.

For the future, the Evolved Strategic System (ESS) is expected to provide a next-generation replacement for the AEHF constellation. One option being considered is to disaggregate the satellite into tactical and strategic variants. The planned sequence is for a prototype phase followed by a fielding phase in 2025 with an initial operational capability 5 years later.

Five of the Milstar satellites (see Fig. 2) that AEHF supersedes are in orbit, launched in 1994 through 2003. Each Milstar satellite serves as a smart switchboard in space by directing traffic from terminal to terminal anywhere on the Earth. The satellite actually processes the communications signal and can link with other



**Fig. 2** Milstar satellite (artist's impression)

Milstar satellites through cross-links. Milstar was the first US military communications satellite with this smart switchboard capability which provides flexibility for users with a reduction in ground controlled switching. The satellite establishes, maintains, reconfigures, and disassembles required communications circuits as directed by the users. Milstar terminals provide encrypted voice, data, teletype, or facsimile communications. A key goal of Milstar is to provide interoperable communications among the users of Army, Navy, and Air Force Milstar terminals.

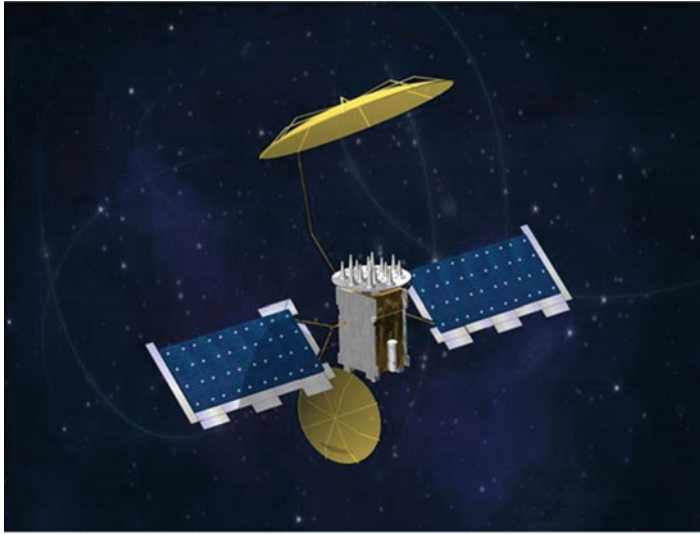
Each Milstar satellite weighs 4.5 t and generates 8 kW of electrical power. They are all in inclined geosynchronous orbit. The cost of each satellite was about \$800 million. Prime contractor was Lockheed Martin Missiles and Space.

The Protected SATCOM Division of the Space and Missile Systems Center's MILSATCOM Directorate is the program office for the AEHF system and is responsible for acquisition of the space and ground segments as well as the Air Force terminal segments. The Army and Navy acquire their own terminals.

The AEHF satellites are operated by the 4th Space Operations Squadron (4 SOPS) located at Schriever AFB, Colorado. The mission control segment controls satellites on orbit, monitors satellite health, and provides communications system planning and monitoring.

## **MUOS and UFO**

The four Mobile User Objective System (MUOS) satellites (plus one on-orbit spare) are designed to replace the ultrahigh frequency (UHF) follow-on (UFO) constellation that provides narrowband communications (64 kbps or less). MUOS (see Fig. 3) is designed to support users that require mobility, high data rates (up to 384 kbps "on the move"), and improved operational availability. A 2012 US Navy information bulletin described the UHF spectrum as "the military's communications workhorse, as it is the most effective military radio frequency for penetrating jungle foliage, inclement weather, and urban terrain on the move." The current UFO constellation comprises eight operational UFO satellites augmented by two pre-UFO FLTSAT



Credit: US Navy

Artist's impression of MUOS in orbit

**Fig. 3** MUOS satellite

satellites and leased services on communications satellites. The UFO satellites achieved initial operational capability in November 1993 and full operational capability in February 2000. The final satellite in the series, UFO-F11, was launched in December 2003.

Each MUOS satellite carries a legacy payload that allows terminals compatible with the UFO system to continue in service. In addition, MUOS carries a payload that provides a military variant of the commercial 3-G wideband cellular service using Wideband Code Division Multiple Access (WCDMA) technology. Fully fielded, MUOS provides an aggregate of 40 Gbps for the military user, compared to the legacy UFO system's aggregate of 2.7 Gbps – a 15-fold increase. The increase means users have more than 16,332 simultaneous accesses (voice, video, data) at 2.4 kbps, compared to 1,111 accesses provided by the UFO satellite system at the same data rate.

User information flows to the satellite via UHF WCDMA links, and the satellites relay this by Ka-band feeder link to one of the four Earth stations in Italy, Australia, Hawaii, and Virginia that are interconnected by a fiber-optic terrestrial network. These facilities identify the destination of the communication and route the information to the appropriate ground site for Ka-band uplink to the satellite and then relay via UHF WCDMA downlink to the correct users. MUOS uses Internet Protocol versions 4 and 6 (IPv4/IPv6) to give users connectivity to the military internet.

The four operational MUOS satellites were launched in 2012, 2013, and 2015 (two launches) and are now in geosynchronous orbit at longitudes 15.5°W,

100°W, 177°W, and 75°E each with an inclination of 5°, plus MUOS-5 as an in-orbit spare in a slightly elliptical orbit with an inclination of about 8° and a longitude close to 108°W (a longitude where minimal East-West station-keeping fuel is required).

The fifth MUOS satellite launched in June 2016 suffered a propulsion failure that prevented it reaching its planned orbit. The Navy ground operations staff used the onboard fuel for station keeping to propel the spacecraft into an orbit that was geosynchronous and with enough fuel left to provide operational utility.

MUOS-1 weighed 6.8 t (15,000 lbs) at its February 24, 2012, launch which was the heaviest satellite ever carried by an Atlas 5 rocket. Like AEHF, the satellite is based on prime contractor Lockheed Martin Space Systems' A2100 platform bus. The solar arrays produce 15.4 kW (end-of-life performance). Overall cost of the five satellites plus associated ground infrastructure was \$7.4 billion.

A key feature of MUOS (and of commercial satellites such as Inmarsat-4, Thuraya and ACES that offer similar services to users on the move) is a large antenna that unfurls in orbit to a diameter of 14 m (46' – almost the width of a basketball court). Each satellite has 16 WCDMA beams: four WCDMA beams on four 5 MHz carriers and UHF channel bandwidths of 17.5 kHz and 21.5 kHz.

The wideband CDMA for communications in motion is intended to be compatible with the Joint Tactical Radio System (JTRS) series, a program that has had a troubled history. In August 2018 MUOS was approved for expanded operational use by US Strategic Command. The Marine Corps will be the first service to widely deploy MUOS, largely due to its 6-year investment in MUOS portable radios. The Marine Corps began initial MUOS fielding to its AN/PRC-117G radios in the fourth quarter of 2018, followed by initial operational capability in the first quarter of 2019. In contrast to the Marines, according to an April 2018 Government Accounting Office report, the Army Handheld, Manpack, and Small Form Fit Radios (HMS) program is not scheduled to enter full production until 2021 – HMS continues efforts begun under the Joint Tactical Radio System.

Once its on-orbit testing has been completed, MUOS is operated by the Naval Satellite Operations Command in Point Mugu, California.

The possibility of selling UHF satellite service to the US military tempted commercial satellite operator Intelsat to build a suitable payload into its IS-27 satellite that was destroyed in a launch vehicle failure 40 s after lift-off in January 2013. Similar commercial “hosted payload” deals have been taken up by defense agencies in several countries including Britain, France, Spain, and Australia.

The USA opened MUOS to international partners in 2015. Canada has requested access to the system and as of late 2018 was in negotiation with the USA over the details of the agreement. Canada had considered co-financing a sixth MUOS satellite with Lockheed Martin but has instead decided to pay the US Government for assured access to the MUOS services.

## Wideband Global SATCOM (WGS)

The Wideband Global SATCOM (WGS – previously called wideband gap-filler satellite – see Fig. 4) offers wideband broadcast and communications services.

The system supports continuous 24-h per day wideband satellite services at X-band and Ka-band to tactical users and some fixed infrastructure users, and it has the ability to cross-band between the two frequencies onboard the satellite. WGS supplements X-band communications that had been provided by the Defense Satellite Communications System III (DSCS-III) and augments the one-way Global Broadcast Service (GBS) satellites through new two-way Ka-band service.

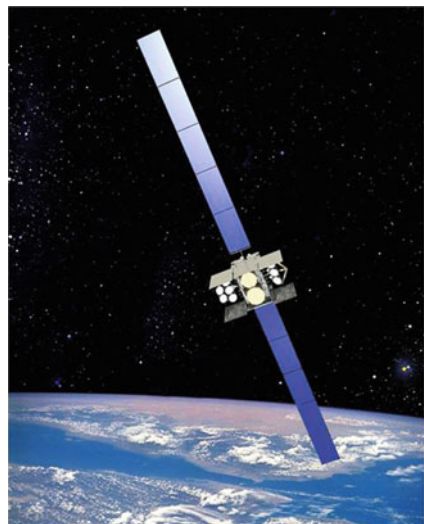
The first WGS in orbit, WGS-1, with its 2.4 Gbps wideband capacity, provided greater capability and bandwidth than all nine DSCS-III satellites combined that it superseded.

The WGS design includes 19 independent coverage areas that can be positioned throughout the field of view of each satellite. This includes:

- Eight steerable and shapeable X-band beams formed by separate transmit and receive phased arrays
- 10 Ka-band beams served by independently steerable, diplexed antennas, including three with selectable RF polarization
- Transmit/receive X-band Earth coverage beams

WGS supports communications links within the government's allocated 500 MHz of X-band and 1 GHz of Ka-band spectrum. Each WGS satellite can filter and route 4.875 GHz of instantaneous bandwidth. Depending on the mix of ground

**Fig. 4** WGS satellite



Credit: USAF

**Artist's impression of WGS in orbit**



terminals, data rates, and modulation schemes employed, each satellite can support data transmission rates ranging from 2.1 Gbps to more than 3.6 Gbps. By comparison, a DSCS-III satellite supported up to 0.25 Gbps.

Prime contractor Boeing has built WGS on its commercial 702 platform, which includes the Boeing xenon ion propulsion system (XIPS) for on-orbit station keeping and station changes. The gallium arsenide solar cells provide about 13 kW of power, and the mass at launch is about 6 t.

Ten WGS satellites have been launched into geostationary orbit in 2007, 2009 (two launches), 2012, 2013 (two launches), 2015, 2016, 2017, and 2019. WGS 4, 5, and 6 comprised the Block 2 version of WGS. WGS-6 launched on August 7, 2013, was funded by the Australian Department of Defense. A total of 12 WGS have now been ordered, and WGS-7 through WGS-10 are the Block 2 follow-on version, with WGS-9 funded by an international consortium comprising Canada, Denmark, New Zealand, Luxembourg, and the Netherlands. The cost of WGS-5 through WGS-7 is about \$350 million each, while WGS-8 and WGS-9 cost about \$55 million more each due to being outfitted with enhancements that boost their capacity by 30%. WGS-11 and WGS-12 were unexpectedly ordered in 2018 when Congress added \$600 million to the DoD budget that had not been requested by the Pentagon. They are likely to be ready to launch in about 2022.

In 2019, Congress approved \$49.5 million for a new DoD budget line for commercial satellite communications. Congressional appropriators took the money from the \$61 million the Air Force had requested for so-called pathfinder initiatives to supplement or replace WGS services. With the addition of a new program line for commercial SATCOM, Congress is forcing DoD to figure out a strategy for the procurement of commercial services.

Spacecraft platform control is performed by the 3rd Space Operations Squadron (3 SOPS) at Schriever AFB in Colorado Springs, Colorado. Payload commanding and network control is handled by the Army 53rd Signal Battalion headquartered at nearby Peterson AFB, Colorado, with subordinate elements A Co. at Fort Detrick, Maryland; B Co. at Fort Meade, Maryland; E Co. at Fort Buckner, Okinawa, Japan; C Co. Landstuhl, Germany; and D Co. Wahiawa, Hawaii.

The sale of WGS satellites and services to countries such as Australia and Canada has been criticized by some in industry as an encroachment of DOD onto commercial territory. Commercial companies such as Paradigm (European) and Xtar (US and Spanish) offer military satellite communications services outside the USA.

## **Data Relay**

The USA has a number of special relay satellites in high orbits so that US surveillance satellites can transmit data to a US ground station no matter where in the world the surveillance satellite is. The relay satellites are either in a geostationary orbit that is always 36,000 km above the equator or an orbit that takes it further north at a similarly high altitude. For this scheme to work, in addition to the relay satellites

themselves, you have to also place special equipment on the surveillance satellites to enable them to communicate with the relay satellites.

The US military and intelligence communities have two sets of relay satellites at their disposal. First is NASA's Tracking and Data Relay Satellite System (TDRSS) which is described in various NASA publications. (The TDRSS page on the NASA website has links to a variety of documents describing the system and satellite: [www.nasa.gov/directorates/heo/scan/services/networks/tdrs\\_main](http://www.nasa.gov/directorates/heo/scan/services/networks/tdrs_main)). The NRO's postulated imaging radar satellites (see section "[Imaging Radar Satellites](#)") are said by some commentators to use TDRSS to get their images back home quickly, but other US military satellites such as the optical surveillance series (see section "[Optical Imaging Satellites](#)") are said to use a military version of TDRSS that civilian commentators usually refer to as Space Data Systems (SDS) but according to information leaked by Edward Snowden to *The Washington Post* is called QUASAR.

According to several commentators, ten QUASAR satellites have been orbited since 1998 into a mix of geostationary and inclined elliptical orbits. Seven, in 2000, 2001, 2011, 2012, 2014, 2016, and 2017, were placed in geosynchronous orbit from where in principle they can serve surveillance satellites as far as 70° north and south, i.e., to the edge of the Arctic and Antarctic regions (the 2012 satellite is said by some civilian analysts to be a replacement for the one launched in 2001). However beyond about 50° north or south, the surveillance satellite in low orbit has increasing difficulty to stay locked on the QUASAR satellite as the line of sight gets closer and closer to the horizon – by the time the surveillance satellite is at 70° north (or south), the QUASAR geosynchronous satellite appears very close to the Earth and is difficult to track. For this reason some of the QUASAR satellites are placed in what is often called an elliptical Molniya orbit named after the Soviet communications satellites that popularized the orbit 40 years ago. A Molniya orbit is high in the sky over the northern hemisphere and low over the southern hemisphere. The Soviets chose this orbit to provide broadcasting and communications to the whole of the Soviet Union many of whose inhabitants live far to the north. The US military chose it for the same reason – to give good coverage of all of the Soviet Union, especially the militarily interesting regions around Murmansk (69° north) and the Bering Strait (67° north) next to Alaska. Out of its 12-h orbit, 8 h will be in the high northern part, so three such satellites can provide continuous 24-h coverage between them. Three QUASAR satellites launched in 1998, 2004, and 2007 are said to be in these Molniya orbits.

## **Interim and Enhanced Polar System (IPS/EPS)**

The Interim Polar System (IPS) provides protected communications (anti-jam, anti-scintillation, and low probability of intercept) for tactical users in the Arctic region. IPS was deployed to meet the demand for protected polar satellite communications to support submarines, aircraft, and other platforms and forces operating in the high northern latitudes that have been steadily increasing over the last 20 years. The

existing IPS payloads provide EHF low data rate (75 bps to 256 kbps) communications to users above 65° north latitude by using satellites in high elliptical orbit. Initial operational capability of the IPS was achieved in 1998 with the first payload, which was launched in 1997 or 1998 and is reported to be still providing uninterrupted service. The second IPS payload was announced as being in orbit in 2007, although it may have been launched some time earlier. The third payload will replace the first payload at an unknown date in order to maintain full operational capability of the system. The satellites that host these IPS payloads are not publicly identified. The IPS payloads are manufactured by Boeing Satellite Systems.

The Enhanced Polar System (EPS) is expected to provide an essential adjunct to the MILSATCOM mid-latitude systems. EPS will provide continuous coverage in the polar region for secure, jam-resistant, strategic, and tactical communications to support peacetime, contingency, homeland defense, humanitarian assistance, and wartime operations. EPS characteristics will include:

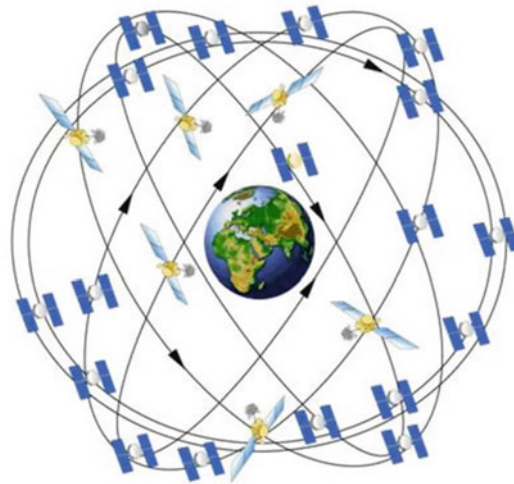
- Protected communications services and communications services without continuous system command and control
- Integrated capability allowing different levels of planners to manage their resources
- Interconnectivity between EPS satellites and mid-latitude users via an EPS Gateway located at a Global Information Grid Point of Presence
- Data rates between 75 bps and 1.28 Mbps (threshold)
- AEHF Extended Data Rate (XDR)-interoperable waveform

The first two operational EPS payloads were delivered by prime contractor Northrop Grumman to the Air Force in 2013 and were placed in orbit on unidentified satellites probably in 2016 and 2017. The initial EPS system comprises two EHF communications payloads hosted on satellites operating in highly elliptical orbits, modified AEHF communications terminals, a gateway to provide connectivity into other communication systems and the Global Information Grid (GIG), and an extension of the AEHF Mission Control Segment (MCS) hardware and software to accommodate EPS. The antenna farm on the payload includes a spot beam aimed at the gateway, a user spot beam, and a user Earth coverage beam. In 2018 Northrop Grumman was awarded a \$429 million contract to provide two Extremely High Frequency eXtended Data Rate (EHF XDR) payloads for the Enhanced Polar System-Recapitalization (EPS-R). As with the EPS payloads, the EPS-R payloads will maintain continuity of protected military satellite communications in the North Polar Region and are designed to enable hosting on a separately procured satellite with other payloads.

---

## **Global Positioning System (GPS)**

The Global Positioning System (GPS) provides accurate and reliable positioning and timing to military and civil users around the world. At a minimum, the GPS constellation needs 24 satellites in six orbital planes (see Fig. 5) in order to ensure



Credit: USAF

**Artist's impression of GPS Constellation (not to scale)****Fig. 5** GPS constellation

that at least four satellites are in view by the user at all times. The constellation flies in a semi-synchronous orbit at approximately 20,000 km above the Earth.

GPS satellites have a semi-synchronous orbit, with a period of 11 h and 58 min. The 2-min offset from 12 h accommodates the movement of the Earth around the sun during a single GPS satellite orbit, i.e., the GPS orbital period is based on a sidereal day and not the solar day.

Due to better than specified reliability in orbit, the current constellation consists of about 30 satellites. The added redundancy offers improved accuracies and availability to users. As of late 2018, the GPS operational constellation comprised 1 Block IIA, 11 Block IIR, 7 Block IIR-M, and 12 Block IIF satellites – the various Blocks will be described below and are summarized in the 2 accompanying diagrams: “GPS modernization program” (Fig. 6) and “GPS program evolution” (Fig. 7). The oldest of the 31 satellites was launched in 1993, and in October 2018, their average age was 11.1 years.

GPS offers two types of services to its user base – the standard positioning service (SPS) and the precise positioning service (PPS). The SPS is available for anyone's use – military or civil. SPS offers 3–5-m accuracy. The PPS can only be accessed by authorized personnel – those with the correct decryption keys such as the US military or its allies. PPS accuracy is 2–4 m. There are several signals and codes that make up each of the GPS services.

Today, GPS transmits on the frequencies L1 (1575.42 MHz) and L2 (1227.6 MHz). The codes transmitted on these frequencies are the coarse acquisition (C/A) code and the pseudorandom (P(Y)) code. Currently, the C/A code is transmitted on L1 and P(Y) is on both L1 and L2. The C/A code is what everyone receives

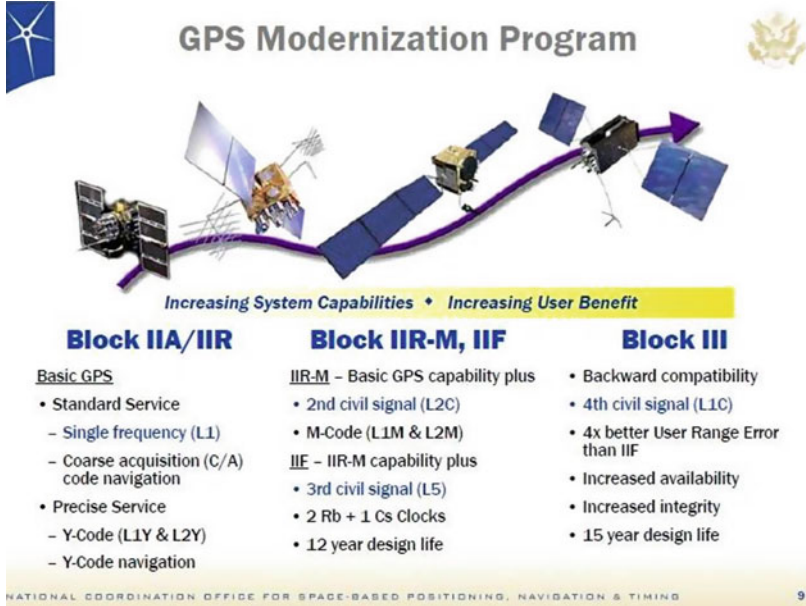


Fig. 6 GPS modernization program

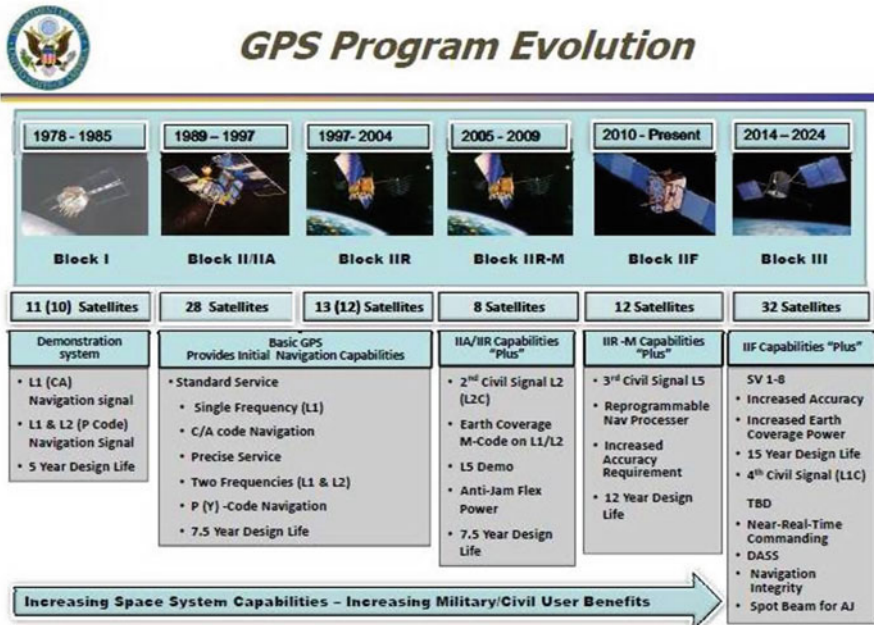


Fig. 7 GPS program evolution

– it is the code within the SPS. The P(Y) is an encrypted code and can only be received by those with the appropriate keys. This is the code that is obtained when a user is subscribed to the PPS.

Block IIA and IIR satellites transmit only two signals and codes – C/A on L1 and P(Y) on both L1 and L2. The Block IIR series are “replenishment” satellites developed by Lockheed Martin. Each IIR satellite weighs 4,480 lb (2,030 kg) at launch and 2,370 lb (1,080 kg) once on orbit. The first attempted launch of a Block IIR satellite failed on January 17, 1997, when the Delta II rocket exploded 12 s into flight. The first successful launch was on July 23, 1997. Twelve satellites in the series were successfully launched.

Within the Block IIR-M, the M-code, a second civil signal (L2C), and flex power have been added. L2C enables civil receivers to correct for the ionosphere. Flex power allows power to be transferred from one signal to another, thus providing some additional anti-jam capability. The first Block IIR-M satellite was launched on September 26, 2005, and the eighth and final launch of a IIR-M was on August 17, 2009. The prime contractor was Lockheed Martin.

The Block IIF series are “follow-on” satellites developed by Boeing and have everything that IIR-M offers but add a third civil signal on L5 (used during “safety of life” applications). Boeing built a total of 12 Block IIF satellites. The first was launched in May 2010 on a Delta IV rocket, and the twelfth on February 5, 2016. The spacecraft has a mass of 1,630 kg (3,600 lb) and a design life of 12 years. Compared to previous generations, GPS-IIF satellites have a longer life expectancy and a higher accuracy requirement. Each spacecraft uses a mix of rubidium and cesium atomic clocks to keep time within eight billionths of a second per day. They provide an improved military signal and variable power for better resistance to jamming in hostile environments.

The average contracted cost of a GPS-IIF satellite is \$121 million although it is reported that Boeing has had to spend \$306 million on each of the first three satellites. The price of the final nine GPS-IIFs was set in 2000.

The most advanced block in production and being deployed is GPS-III. It has all the same capabilities as IIF and many added capabilities. It has increased power in the form of a spot beam, and it has slightly better accuracy, mostly due to cross-links that greatly reduce the age of data. Each GPS-III also carries three improved rubidium clocks and transmits four civil signals: L1 C/A, L1C, L2C, and L5. Each spacecraft weighs 8,115 lbs (3,681 kg) at launch and 4,764 lbs (2,161 kg) when on-orbit. The first was launched in late 2018 (a slip of 4 years since the program evolution diagram above was published). That was also the first GPS satellite launched on the SpaceX Falcon 9 rocket – as of late 2018, SpaceX had won five of six GPS-III launch contracts so far awarded, the first for a price of \$83 million, the others \$97 million each (about one quarter the price of the United Launch Alliance rockets used for earlier GPS launches).

Lockheed Martin received a \$1.5 billion contract to develop the first two GPS-IIIs, followed by a \$2.1 billion extension for satellites three through eight (\$350 million each) and a \$395 million extension for satellites nine and ten (\$200 million each). In September 2018 Lockheed Martin was selected to build 22 GPS-IIIF

(follow-on) satellites at a price of \$7.6 billion (\$345 million per satellite). Additional features include a 100% digital navigation payload, Regional Military Protection, and new search-and-rescue payloads. Further features may be added at three “technology insertion points” in the GPS-III program beginning with satellites 7, 13, and 19, respectively. The first launch of a GPS-III satellite is scheduled for 2026, with the last foreseen in 2034. The GPS-III satellites are all built on the Lockheed Martin A2100 commercial satellite platform with refinements such as additional radiation shielding to ensure the required 15-year lifetime in the medium Earth orbit (MEO) where the radiation environment is less benign than in geostationary orbit where most A2100s are located.

The headquarters for the control segment is the master control station (MCS) at Schriever AFB in Colorado Springs, operated by the 2nd Space Operations Squadron (2 SOPS) of the 50th Space Wing of the US Air Force. In addition to the master control station, there are six dedicated GPS monitoring stations and ground antennas, located at Colorado Springs, Kwajalein Atoll, and Hawaii in the Pacific Ocean, Ascension Island in the Atlantic Ocean, Diego Garcia in the Indian Ocean, and Cape Canaveral in Florida.

GPS satellites are commanded and controlled via the monitor stations, the MCS, and the ground antenna. Monitor stations are essentially high-quality GPS receivers placed at various precise locations throughout the world. These receivers track the satellites just like a normal receiver would – they obtain the satellites’ ephemeris and any downlinked data. Information is then transferred to the MCS where it is processed to calculate the orbit and clock offsets of each satellite. The MCS transmits that data back to the satellite via the ground antenna to update the satellite with its true location and time. These upload corrections occur at least once per day, although the system can operate autonomously for an extended period if necessary – albeit with reduced accuracy.

To give a snapshot of the scale of the US military commitment to GPS, the US Congress appropriated \$1.4 billion for it in FY2019 which included \$451 million for GPS-III satellites. \$513 million was for the accompanying ground system, the centerpiece of which is a next-generation ground control system, called OCX, that has been plagued by delays, prompting the Air Force to pump more money into upgrading the existing GPS system as a stopgap. The DOD request to Congress for FY2020 includes \$1.7 billion for GPS satellites and its ground system and user terminals.

A \$1.5 billion OCX contract was awarded to Raytheon in 2010 to develop and deploy a major new version of the GPS control segment. The initial OCX capability was expected to be online in 2015, but additions and extensions have pushed that date back to the early 2020s, with costs rising to about \$6 billion. Because of the delays to OCX, Lockheed Martin received a \$96 million contract modification in 2016 to adapt the existing GPS ground system so that it provides a stopgap level of support for the GPS-III satellites that would allow them to be launched. Because of delays to the launch of the first GPS-III, the Block 0 version of OCX (known as the Launch and Checkout System, LCS) was deployed to support that launch.

## Surveillance

### Introduction

Large elements of the US military surveillance satellite capability are classified, and the information in this chapter is drawn only from unclassified sources with the inevitable risk that the information is incomplete or wrong. The scale of the programs is enormous, including what the Head of the National Reconnaissance Office described as “the world’s largest satellite.” The following is the breakdown of the topic in this section:

- Optical Imaging Satellites (Section “[Optical Imaging Satellites](#)”)
- Imaging Radar Satellites (Section “[Imaging Radar Satellites](#)”)
- Missile Early Warning Satellites (Section “[Missile Early Warning Satellites](#)”)
- Nuclear Detonation Detection Systems (Section “[Nuclear Detonation Detection System](#)”)
- Signals Intelligence Satellites – non-Maritime (Section “[Signals Intelligence Satellites: Non-maritime](#)”)
- Maritime Signals Intelligence Satellites (Section “[Maritime Signals Intelligence Satellites](#)”)
- Weather Satellites (Section “[Weather Satellites](#)”)

### Optical Imaging Satellites

Since the 1980s the US military has relied on a series of surveillance satellites referred to by the media as Keyhole satellites although the name for the more recent satellites is Enhanced Imagery System (EIS). They are large expensive spacecraft, each weighing 10–15 t and costing about \$1.5 billion (of which a third is for the launcher) – one was said by NRO to have cost \$2 billion less than originally projected, which suggests a multibillion dollar price tag. They orbit at between 250 and 1,000 km altitude and provide optical images that are said to have a resolution of 8–10 cm (3–4 in.) and less detailed infrared images. There are thought to be seven in orbit in early 2019 launched in 1995, 1996, 2001, 2005, 2011, 2013, and 2019, and there must be some doubt about whether the two older ones are still fully functional. The four launched in 2001 through 2013 are upgraded versions that provide very wide coverage as well as detailed images. They can rotate their camera to dwell on a scene as they pass across the sky. The infrared feature means that they can take nighttime images.

General Bruce Carlson (see Fig. 8) when he was the Director of the National Reconnaissance Office that buys and operates these satellites promoted a cost-saving concept called Next-Generation Electro-Optical reconnaissance satellite or NGENEO. He said that it “will require a little bit of up-front investment” but will result in a modular and flexible satellite allowing NRO to insert new technology more rapidly than at present as well as reducing costs. He was determined to halt the “erosion in



**Fig. 8** Gen. (retired) Bruce Carlson



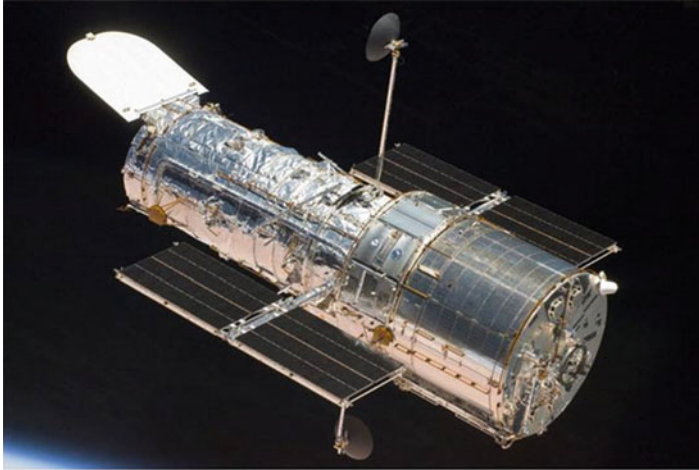
Credit: NRO  
NRO Director Gen. Bruce Carlson

the [NRO's] science and technology base" that he described as "the seed corn for the future." Improving the technology to put into its expensive operational satellites is also addressed using tiny low-cost "CubeSats." NRO had 12 CubeSats under construction in 2009 according to NRO official Karyn Hayes-Ryan. She noted that they can be built in less than 6 months and thus enable NRO to "keep pace with Moore's law." Batteries, solar cells, computer processors, gyroscopes, and radios were some of the technologies she listed as being tested on CubeSats. As well as quickly and cheaply testing new ideas in space, this approach helps train people and is "more risk tolerant" according to Ms Hayes-Ryan. Two launches in 2013 carried a total of 40 NRO-related CubeSats into orbit.

General Carlson noted that many of the current satellites have lasted far longer than expected, and they deliver useful intelligence mainly because of "the young people that write software" to adapt the images the satellites produce. He joked that "we have satellites inside our very aging constellation that are old enough to vote and some, that are still operating, are old enough to drink. We don't let them drink, but they are old enough to drink." On another occasion he quipped that "half the constellation is geriatric." He pointed out however that because of the improvements in software "if you look at the product that we got ten years ago and compare it to the product that we have today, in many cases, it's an order of magnitude better in quality whether it's accuracy or clarity or timeliness."

An eighth satellite similar to the seven just mentioned may also be in orbit at about 800 km altitude and is said to be a stealth satellite, impervious to detection from the ground. Launched in 1999 it was part of a program called MISTY that is thought to have to been cancelled in 2006 when projected costs got out of hand. Intelligence specialist Jeffrey Richelson who first broke the story about the MISTY satellites is skeptical about their stealthiness. He notes that civilian observers were able to keep track of the first MISTY satellite launched in 1990 and watch its various maneuvers.

The EIS satellites are thought to resemble the Hubble Space Telescope (see Fig. 9) in shape and size, and are supplied by the same prime contractor, Lockheed Martin. This suggested resemblance was reinforced in 2012 when the NRO donated



Credit: NASA photo

## Hubble Space Telescope in orbit

**Fig. 9** Hubble space telescope

two unused optical assemblies (essentially telescopes) to NASA similar in size to those of Hubble. The telescopes are thought to have been left over from the cancelled program to develop a replacement for the EIS satellites, called the Future Imagery Architecture. The telescopes weigh 1.7 t each and have the same sized primary mirror as Hubble, 2.4 m diameter, but lack cameras (detectors, filters, prisms, etc.), stabilization, power, and so on. They have a wider field of view than Hubble, and the optical quality of the mirror surface is not too dissimilar – about 60 nm versus Hubble’s 30 nm. Budget figures leaked by Edward Snowden indicate that development of a new series of satellites began in 2012 called the Evolved Enhanced CRYSTAL System (EESC) – NROL-71/USA-290 launched in early 2019 is said by some analysts to be the first of this new series of imaging spy satellites. Unofficial orbital information puts it in a 400-km near-circular orbit inclined at 73.6°. The leaked funding figures also suggest that production of EIS satellites is being run down.

The US military has been a major purchaser of commercial satellite images (such as those of France’s SPOT series) for many years. In 2003, the National Geospatial-Intelligence Agency (NGA) placed two contracts guaranteeing to purchase \$150 million per annum of imagery from each of two suppliers and offered about half of the \$500 million cost of building and launching each of the high-resolution optical satellites. The action by NGA followed on from a \$100 million contract for high-resolution imagery in 1999 to a third company. A smaller contract followed in 2004 to that third company, and in 2005 that company merged with one of the 2003 winners leaving DigitalGlobe and GeoEye as NGA’s two high-resolution commercial suppliers. In 2010 the NGA reinforced its commitment to using commercial imagery with the award of contracts valued at \$7.3 billion in total over 10 years

to the two companies, although cutbacks driven by the Federal budget deficit reduced the per year value of these contracts somewhat, partially as a consequence of which the two companies combined in 2013 under the name DigitalGlobe. In 2018, NRO assumed responsibility for the NGA contract and then awarded DigitalGlobe a \$900 million extension to provide commercial imagery until August 2023. DigitalGlobe supports the NRO with three satellites – WorldView-1, WorldView-2, and WorldView-3. WorldView-4 (launched in 2016) was to have been available should there be any interruptions or degradation in the performance of the earlier satellites (ground resolution of 30 cm is achievable) but stopped producing usable imagery in early 2019 due to failure of its control moment gyros. The company is building a \$600 million WorldView Legion constellation, which will comprise at least three satellites, with the first scheduled to launch in 2021.

The formation of the NRO as a joint venture of the DOD and the CIA illustrates that the data from imaging satellites is used by two distinct communities – the military and the intelligence agencies. The friction between the requirements of the two communities surfaces from time to time, e.g., the urgent, tactical needs of the military in today’s conflict zone versus the background gathering of information about tomorrow’s enemy by the intelligence agencies. Budget pressures are said to have increased this tension and even to have contributed to the relatively early retirement of General Carlson as NRO Director.

The NGA, with a budget of about \$5 billion per annum, is the arm of the military and intelligence communities that “develops imagery and map-based intelligence solutions for US national defense, homeland security, and safety of navigation.” In other words they process the imagery from spy satellites.

## Imaging Radar Satellites

In the summer of 2008, the US Administration declassified the fact that the country has radar imaging satellites. This was hardly Earth-shattering news since the “secret” had been widely known and discussed for more than a decade. It is also common knowledge that US efforts to develop a new generation of imaging radar satellites had become so expensive that the effort was cancelled in 2008. Perhaps this more cost conscious approach explains why the number 2 official at the NRO, Betty Sapp, was able to tell a Congressional Subcommittee in April 2010 that “the NRO received an Unqualified Opinion on its fiscal year 2009 Financial Statement.” More surprisingly, she added that “this was the first clean audit for a defense intelligence agency since 2003.”

As of late 2018, some analysts consider that there are five of the most recent generation of radar satellites in orbit, produced by Lockheed Martin. These Topaz satellites (often called “Lacrosse” or sometimes “Onyx” by the media) are thought to weigh about 4 t and are extremely large (50 m across with their solar arrays deployed) in order to generate the 10–20 kW of power needed to drive the radar – and correspondingly expensive at \$1½ billion each. They provide imagery through cloud and in the dark with a resolution of about 1 m. They orbit at about 1,000–1,100 km altitude with orbital inclination of about 60° (or 120°), while earlier

models orbited about 400 km lower and were considerably heavier (14 t). Ground-based imagery taken by amateur observers appears to show a gold-colored circular or ellipsoidal radar dish of about 50 m diameter – probably with a mesh surface rather than a solid one. Leaked budget figures show that procurement of a Block 2 series of the Topaz satellites began in 2013.

The USA has turned to the international commercial marketplace to augment the Topaz radar images. In 2008, the NGA began to buy small quantities of radar imagery from Canadian company MDA which owns and operates the Radarsat satellites. Then in early 2010, the NGA placed contracts to buy up to \$85 million worth of data over a 5-year period from each of the three foreign imaging radar satellite families: Germany's TerraSAR-X and Tandem-X, Italy's four COSMO/SkyMed satellites, and Canada's Radarsat-1 and Radarsat-2. The US Southern Command has also purchased some Israeli TecSAR imagery probably to help in the war on drugs in Central and South America.

## Missile Early Warning Satellites

For more than 40 years, the US satellites used to spot missile launches (also called early warning satellites) have been labeled as Defense Support Program (DSP) satellites. These have now been replaced by the Space-Based Infrared System (SBIRS).

The first DSP was launched in November 1970, although a series of experimental satellites, with the designations MIDAS and RTS, had been launched throughout the 1960–1966 period to demonstrate the concept of launch detection and try out various techniques – different orbits, sensors, data recovery methods, and so on. The general idea was to watch for the bright flash of light and flare of heat given off by a rocket motor. They proved very successful at spotting Soviet and Chinese missile launches. DSP data allowed the launch site to be pinpointed to within 3–15 km and the launch heading to within 5–25° depending on various factors such as the relative location of the launch and the DSP satellite. There were a few false alarms but only for smaller missiles such as submarine-launched missiles in the northern hemisphere summer (due to the glint of the sun on the sea).

Any bright flash triggered the DSP sensors, but software algorithms sorted out the missile launches from ammunition dump explosions, forest fires, gas pipeline fires, the burnup of satellites reentering the Earth's atmosphere, and military jet aircraft using afterburner – even the July 1996 explosion of TWA Flight 800.

As the capabilities of DSP satellites have grown, so have their weight and power. Unlike the old lightweight, low-power satellites, the newest generation of DSP satellites weighs over 5,000 lb, and the solar arrays generate 1,285 W of power. The most recent DSP satellite is approximately 33 ft long and 22 ft in diameter. The system comprises the satellite vehicle, also referred to as the bus, and the sensor. The satellites are placed in geosynchronous orbit. Global coverage can be efficiently achieved with three satellites. Additional satellites can provide dual or triple coverage, providing for more accurate and timely event reporting.

The DSP satellite spins around its Earth-pointing axis, which allows the infrared (IR) sensor to sweep across each point on the Earth.

The DSP sensor detects sources of IR radiation. A telescope/optical system and a photoelectric cell (PEC) detector array, comprised primarily of lead sulfide detectors and some Mercad-Telluride cells for the MWIR detection capability, are used to detect IR sources.

The SBIRS replacements for the DSP missile warning satellites are now in orbit. The first two elements of the highly elliptical orbit (HEO) part of the SBIRS constellation were launched in 2006 and 2008, piggybacking on other unidentified (for security reasons) US military satellites. The third and fourth SBIRS HEO payloads have also been launched – some analysts have identified NRO payloads USA-259 launched on December 13, 2014, and USA-278 launched on September 24, 2017, as their host spacecraft. Four SBIRS have been launched into geosynchronous orbit in 2011, 2013, 2017, and 2018. Two more (GEO-5 and GEO-6) are in production, due to be launched in 2021 and 2022. Lockheed Martin Space Systems in Sunnyvale, CA, is the SBIRS prime contractor, with Northrop Grumman Electronic Systems in Azusa, CA, as the payload subcontractor, and Lockheed Martin Information Systems and Global Services in Boulder, CO, as the ground system subcontractor.

The technology used in SBIRS is much more powerful than in DSP. Unlike DSP, the output of the sensor is an image not just a location, so further analysis can be performed on it.

The GEO spacecraft bus consists of a militarized, radiation-hardened version of the Lockheed Martin A2100 spacecraft, providing power, attitude control, command and control, and a communications subsystem with five separate mission data downlinks to meet mission requirements. The GEO infrared payload consists of two sensors: a scanner and a step-starrer. The scanning sensor continuously scans the Earth to provide 24/7 global strategic missile warning capability. Data from the scanner also contributes to theater and intelligence missions. The step-starring sensor, with its highly agile and highly accurate pointing and control system, provides coverage for theater missions and intelligence areas of interest with its fast revisit rates and high sensitivity. Similar to the GEO scanning sensor, the HEO sensor is a scanning sensor, with sensor pointing performed by slewing the full telescope on a gimbal. Both the GEO and HEO infrared sensors gather raw, unprocessed data that are downlinked to the ground, so that the same radiometric scene observed in space will be available on the ground for processing. The GEO sensors also perform onboard signal processing and transmit detected events to the ground, in addition to the unprocessed raw data.

The GEO satellite weighs 5,525 lbs (2,506 kg) in orbit including the 1,100 lbs (499 kg) two-sensor payload and 430 lbs (195 kg) of fuel. The HEO sensor payload weighs 530 lbs (240 kg).

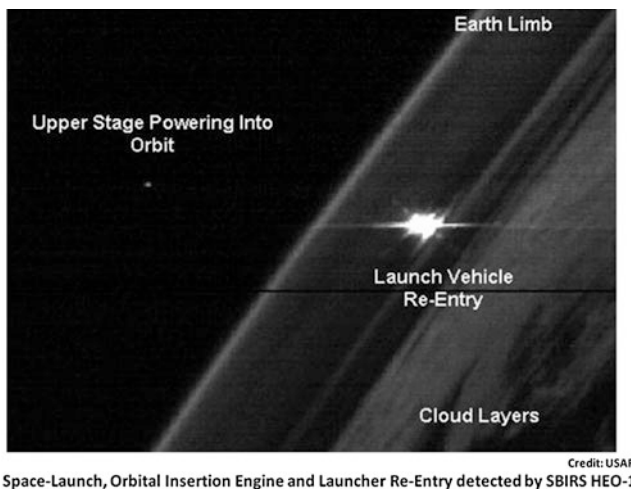
The sophistication of the facilities on the ground has also been enhanced – more powerful computer processing to analyze the information and faster relaying of results to the troops, ships, or planes that can do something about it. Even before the first SBIRS was launched, the timeliness and quality of DSP information had

improved because of this. One industry official claims SBIRS will be ten times better than DSP, able to detect dimmer and more fleeting targets, and presumably the effects of the upgraded ground facilities will improve that even further.

The second SBIRS piggybacking on an unnamed military satellite is also sending back high-quality information. Figure 10 shows the track of a missile above the clouds as seen by SBIRS, indicating that the trajectory can be spotted and analyzed in quite some detail.

Already 7 years behind schedule, the first geosynchronous SBIRS satellite fell foul of a very modern problem in 2009 in that its software was found to be faulty, resulting in a delay and modification that cost \$750 million. The faults were so bad that USAF Colonel Robert Teague said “the [software] design and architecture had fundamental flaws. The solution essentially required starting from scratch.” General Robert Kehler, the head of the USAF Space Command, sounded resigned to even more delays and cost increases when in the fall of 2009 he said that “I don’t know if there will be any other impacts to schedule and cost. I’m not optimistic or pessimistic. We are where we are with SBIRS.” What is now considered to be the full constellation of two geosynchronous and two elliptical satellites costing about \$15 billion was due to be operational in 2014, but the system won’t achieve full use of any GEO satellite staring sensors until the ground systems are modified, around 2018.

SBIRS is an integrated “system of systems” consisting of ground components as well as the satellites described above. The ground component consists of control stations such as the Mission Control Station located at Buckley AFB, Colorado, which is responsible for consolidating event data from dispersed legacy DSP ground systems. Remote ground stations (including mobile and deployable stations) receive missile warning data from the satellites and feed the data via secure communications



**Fig. 10** SBIRS HEO-1 Image

links to ground stations for processing. The ground stations assess system reliability, attempt to identify the type of launch occurring, and generate a launch report. Crews send these reports to the NORAD operations centers at Cheyenne Mountain AFS, Colorado; the Alternate Missile Warning Center at Offutt AFB, Nebraska; and other command centers. Air Force Space Command's 460th Operations Group is responsible for conducting HEO, GEO, and DSP operations at all fixed ground sites.

Because of the lengthy delays and cost overruns in deploying the SBIRS satellites, an alternative approach was begun leading to the launch of a flight demonstrator in September 2011. The Commercially Hosted Infrared Payload (CHIRP) was hosted on the geostationary commercial telecommunications satellite, SES-2, developed by Orbital Sciences. The sensor payload was supplied by SAIC of McLean Virginia. CHIRP is a wide field of view staring sensor designed to detect and track the heat signature of missiles at launch. The budget of \$216 million is considerably lower than the >\$1 billion budget for the SBIRS satellites, but now that those are finally being deployed, the CHIRP concept seems likely to be discontinued.

In May 2018 the planned purchase of two further geosynchronous SBIRS satellites (GEO-7 and GEO-8) was cancelled and a plan announced to buy three upgraded geosynchronous Overhead Persistent Infrared (OPIR) satellites from Lockheed Martin and two polar-orbiting spacecraft from Northrop Grumman. Northrop was awarded \$47 million to begin analysis and risk reduction work for the first two polar-orbiting satellites, while Lockheed Martin was authorized to begin up-front work on a potential \$2.9 billion contract. Fiscal Year 2019 funding for OPIR was \$806 million, and the FY2020 request to Congress was for \$1.6 billion. The satellites are scheduled for launch on a rapid time line, with the first in 2023. The planned constellation is due to be in place by 2025, 4 years earlier than the original plan for an Evolved SBIRS.

## **Nuclear Detonation Detection System**

The GPS satellites described in section “[Global Positioning System \(GPS\)](#)” carry an additional payload suite to support a nuclear detonation detection system (NDS). The NDS payload is also carried by the DSP early warning satellites described above (which are gradually being phased out) and was initially the primary mission of the VELA satellites. The sensor array includes optical, x-ray, dosimeter, and electromagnetic pulse (EMP) sensors which detect and measure light, x-ray, subatomic particle, and EMP phenomenology to pinpoint the location and yield of a surface or airborne nuclear detonation. A nuclear explosion starts off with a short very intense flash and then a short dimming while expanding gas overtakes the fireball and masks it from view until the gas has thinned and cooled enough for the fireball to be visible again – this dual flash enables the NDS to distinguish a nuclear explosion from other events. The information sensed on the GPS NDS system is relayed to the ground-based Integrated Correlation and Display System (ICADS) via a dedicated channel,

L3 (1381.05 MHz). NDS supports several tasks, such as treaty monitoring and nuclear force management.

GPS-III satellites carry a newly designed nuclear detection payload, details of whose performance are classified.

## **Signals Intelligence Satellites: Non-maritime**

The first US communications intelligence (COMINT) satellite was launched in 1968. Called CANYON it was the first of a series that is thought to continue today although the name has changed over the years – to CHALET then VORTEX then MERCURY and currently NEMESIS and ORION. The name changes were to some extent caused by security lapses such as that by British spy (and pedophile) Geoffrey Prime and US spy Christopher Boyce.

The technology of these eavesdropping satellites is impressive. They are located 36,000 km out in space in the geostationary arc. Being so far from the ground, the satellites need enormous radio antennas to pick up radio signals. The MUOS antenna (see section “[MUOS and UFO](#),” above) is 14 m in diameter when unfurled in orbit. But the secret eavesdropping satellites are thought to have already been 50 m wide by 1994 and 90 m by 2006 – at least one newspaper report claimed they had dishes 150 m wide (almost 500 ft). The Head of the NRO, General Bruce Carlson, said that the satellite launched on November 21, 2010, from Cape Canaveral was “the largest satellite in the world” – thought to be one of the ORION series mentioned below.

The first satellite to “watch” the Earth was in fact an electronic intelligence (ELINT) satellite – the tiny GRAB satellite. GRAB was launched into orbit in 1960 and provided hitherto inaccessible information about radar systems deep inside the Soviet Union. GRAB worked by receiving radio signals across a very wide range of frequencies and relaying them to a station on the ground. The satellite didn’t process the signals in any way, just acted like a “bent pipe” in taking radio signals that it heard at its 1,000 km altitude and beaming them downwards to a friendly station. By having a station suitably located near the border, signals from 5,500 km inside the Soviet Union could be picked up. Signals from two Soviet radar systems, one associated with SAM-1 anti-aircraft missiles and the other with missile early warning, were detected and could then be analyzed. The advantage of knowing the characteristics of an adversary’s radar was not only that you could in future know what it was when you detected it, but you could design electronic countermeasures to jam it or confuse it. GRAB was the first of a long line of what became known as ELINT satellites.

The success of GRAB encouraged the USA to use satellites extensively for analyzing its enemy’s radars and other military signals. The tiny GRAB evolved into massive satellites with enormous antennas as discussed above. Many of these satellites were placed in geostationary orbit, 36,000 km above the Earth, hence the need for their giant antennas. One series already mentioned above, initially targeting communications intercepts, began with the launch of CANYON in 1968 which evolved a decade later into CHALET. A second series that was targeted at data



from missile tests began in 1970 with the launch of the first RHYOLITE satellite (later renamed AQUACADE). (The names of US spy satellites are always written in uppercase – the reason for this pretentious habit is not known to the author.) This series evolved to pick up communications transmitted across the Soviet Union via microwave towers. It was succeeded in 1985 by the first of two MAGNUM satellites. In 1994 a new generation of satellites began to appear. As we approach the present day, details about the current US eavesdropping satellites become more and more vague.

In addition to satellites in geostationary orbit, another group of eavesdropping satellites has been picking up radio signals in what is called a Molniya orbit discussed in section “[Data Relay](#)” – this is an elliptical orbit that is at its maximum height over the northern hemisphere and at its lowest over the southern. Their maximum height is similar to a geostationary satellite with a correspondingly broad view of the Earth below. The big advantage is that they cover northern latitudes better than from geostationary orbit, but the disadvantage is that they move along their orbit from north to south and thus are over the northern area of interest only for 8 or so hours a day. Three satellites in Molniya orbit are sufficient to provide continuous coverage over a given area. Initially called JUMPSEAT satellites, these evolved into the TRUMPET satellites that were launched in 1994, 1995, and 1997. The first in what is said to be a TRUMPET replacement series was launched in 2006. Launches on December 13, 2014, and September 24, 2017, carried payloads that may be part of this series.

There are thought to be about a dozen operational US COMINT satellites of this type currently in orbit. Leaked 2011–2013 budget documents list three series called RAVEN (unfunded since before 2011), NEMESIS (unfunded in 2012 and 2013), and ORION. Recent launches of satellites that fall into one or other of the COMINT categories are said to include NRO-26 in January 2009, NRO-32 in November 2010, NRO-15 in June 2012, and NROL-37 in June 2016.

The cost of these satellites is astronomical. Press reports of the January 2009 launch of the 6 t NRO-26 referred to it as a “highly upgraded ORION electronic eavesdropping satellite” and said that “the combined cost of the spacecraft plus booster is roughly \$2 billion.” Leaked budget documents show that a “SIGINT High Altitude Replenishment Program (SHARP)” is underway costing about \$800 million per annum. This suggests that the satellites that emerge from this program will continue to cost in excess of \$1 billion each. The NROL-67 launch on April 10, 2014, may have been one of the satellites from this program. Recent cost overruns of several types of US spy satellites have become public knowledge, and ELINT satellites are no exception. An attempt to move to a more cost effective approach was discussed in the trade press for several years and would have involved a larger number of cheaper satellites – but it seems to have been a failure, since the large expensive type is still being launched every 2 or 3 years.

The high cost of these monster satellites means that they are designed to last for 15 or more years – it would be too expensive to replace them more frequently. But communication is an area which changes dramatically every few years, so the

expensive long-lasting satellites risk becoming obsolete before they have served their term.

## **Maritime Signals Intelligence Satellites**

The USA has for many years deployed constellations of satellites in orbit groups of two, three, or four satellites so that they could triangulate the signals from a ship using the different time and direction of the ship's radio signals as seen by each satellite in the group. The various series of US satellites originally had friendly names (at least for use publicly) starting with Poppy in the 1960s and then White Cloud in the 1970s and 1980s. More recently these satellite groups are referred to as NOSS (Naval Ocean Surveillance Satellite) followed by a -1, -2, or -3 to signify which generation (White Cloud being NOSS-1), and the program has the unfriendly official name, INTRUDER.

Pairs of satellites (the USAF designates one of them as "debris" presumably in an attempt to disguise their mission) launched as NRO-34 in April 2011, NROL-36 in September 2012, NROL-55 in October 2015, and NROL-79 in March 2017 are said to be members of the NOSS-3 series.

A pair of NOSS satellites, each weighing about 3 t, plus the rocket on which they are launched into orbit costs about \$600 million – there are thought to be 20 or so in orbit altogether, spaced so as to give as near as possible continuous coverage of the ocean areas of interest. A database of all ship movements is maintained based on NOSS information plus data from Navy and Coast Guard air and sea surveillance. Civilian as well as military ships are tracked reflecting the threat from terrorists and the interest in the navies of countries such as China and Iran.

In addition to detecting ships and working out their exact location by triangulation, these satellites allow the ships' radar signals and radio communications to be collected for later analysis. In recent years the US military have acknowledged that specific launches are in the NOSS category but not that they are a group – civilian observers have detected additional objects close to the acknowledged one, but the military refer to those objects as "debris." The current INTRUDER (NOSS-3) satellites come in pairs as has been recorded by many ground-based observers just by watching them with binoculars. The satellites are 1,000–1,200 km high with an orbital inclination of about 63° and one of the pair trails the other by 50–250 km. The height is a compromise between being as close to the Earth as possible in order to detect faint emissions and being as high as possible to get a broad view. The relatively small separation of the pair ensures that they both see the same target, thus allowing the signals to be compared and the target's location and direction to be triangulated.

There is occasional press and web speculation that INTRUDER satellites possess radars of their own and thus detect ships that are observing radio and radar silence. Other reports say that INTRUDER satellites can detect the faint radio emissions from a ship's engines and the magnetic effects of a ship's hull.

## Weather Satellites

The Defense Meteorological Satellite Program (DMSP) has been providing weather information for the Department of Defense for half a century (initially it was called Program 35).

Two primary operational DMSP satellites are always in near-circular, sun-synchronous, 835 km altitude, near-polar orbits with a period of 101.6 min and an inclination of 98.75°. The primary weather sensor on DMSP is the Operational Linescan System, which provides continuous visual and infrared imagery of cloud cover over an area 1,600 nautical miles wide (see Fig. 11). Global coverage of weather features is accomplished every 14 h providing essential data over data-sparse or data-denied areas. Additional satellite sensors measure atmospheric vertical profiles of moisture and temperature. Military weather forecasters can detect developing patterns of weather and track existing weather systems over remote areas, including the presence of severe thunderstorms, hurricanes, and typhoons.

The DMSP satellites also measure space environmental parameters such as local charged particles and electromagnetic fields to assess the impact of the ionosphere on ballistic-missile early warning radar systems and long-range communications. Additionally, these data are used to monitor global auroral activity and to predict the effects of the space environment on satellite operations.

DMSP-5D3-F18 was launched in 2009 on an Atlas V 401 and DMSP-5D3-F19 in 2014. Compared with earlier versions, the current Block 5D-3 satellites include upgraded instruments, increased power capability, improved on-orbit autonomy



Credit: USAF  
DMSP's Operational Linescan System produces day & night visual & infrared imagery, such as this night-time view of East Asia showing Japan (right), S Korea (centre) with N Korea almost entirely dark above it, and China (left)

**Fig. 11** DMSP image of East Asia

(60 days), enhanced design-life duration of 5 years, solid-state data recorders, and a UHF downlink which enables data to be sent directly to tactical users. DMSP-5D3-19 suffered a failure of its onboard command and control system in February 2016 and was declared a complete loss in July that year. DMSP-5D3-17, launched in 2006, was reinstated as the second operational unit together with DMSP-18. The only remaining unlaunched DMSP is now in a museum, Congress having cancelled funding to store it in flight-ready condition. The fragile condition of old DMSP satellites was illustrated in February 2015 when the defunct DMSP-5D2-F13 launched in 1995 spun off a large number of pieces of debris, probably due to a battery explosion.

The next-generation DMSP military weather satellites and civilian National Oceanic and Atmospheric Administration (NOAA) satellites were to have been merged into the National Polar-orbiting Operational Environmental Satellite System (NPOESS). In 2010, with \$6 billion having been spent on NPOESS already and the total budget still rising, the program was cancelled. The DOD initiated the Defense Weather Satellite System (DWSS) to replace it, but in 2012 that too was cancelled due to budget constraints.

The DMSP 5D-3 satellites weigh 1¼ ton of which 350 kg is the sensor payload, and the solar panels produce 2.2 kW of power. The satellites are over 7 m long with solar panels deployed.

As a near-term alternative to DMSP, in September 2018 the Air Force awarded a \$119 million contract for the Operationally Responsive Space-8 (ORS-8) satellite to Sierra Nevada Corp. ORS-8 will be an experimental satellite providing cloud characterization and theater weather imagery and will be launched in 2022. As of early 2019, this contract was on hold following a protest by Space Systems Loral (a Maxar Technologies company).

Longer term, two series of Weather System Follow-on (WSF) satellites are envisaged – one carrying mainly microwave instruments and the other carrying mainly optical and infrared instruments. Ball Aerospace received a \$94 million contract in November 2017 to design and develop the WSF Microwave satellite, with options to construct two flight models for a total contract value of \$458 million, with the first to be launched in the 2022–2024 period. A request for information to industry for the WSF electro-optical infrared (WSF-E) satellite was issued in November 2017, envisaging launch of the satellite in 2023 or 2024.

As part of the NPOESS convergence plan, DMSP operations were transferred from the Defense Department to the Commerce Department in 1998, with funding responsibility remaining with the Air Force. Satellite operations were moved to Suitland, MD, where NOAA's Office of Satellite Operations provides the command, control, and communications for both DMSP and NOAA's Polar-orbiting Operational Environmental Satellite System. Although NPOESS has been cancelled, NOAA continues to operate the DMSP satellites using a common civil/military ground system.

Tracking stations at New Boston Air Force Station, NH; Thule Air Base, Greenland; Fairbanks, Alaska; and Kaena Point, Hawaii, receive DMSP data and electronically transfer them to the Air Force Weather Agency at Offutt Air Force Base,

Nebraska. Tactical units with special equipment can also receive data directly from the satellites.

The Space and Missile Systems Center at Los Angeles AFB, California, is responsible for development and acquisition of DMSP systems. The ORS-8 spacecraft procurement is managed by the Space Rapid Capabilities Office (part of Air Force Space Command) at Kirtland Air Force Base, NM.

---

## Other Satellites

### Space-Based Space Surveillance (SBSS)

The first Space-Based Space Surveillance (SBSS) satellite was launched in 2010 able to detect debris, spacecraft, or other distant space objects without interference from weather, atmosphere, or time of day. SBSS is especially useful for monitoring small objects in geostationary orbit – ground-based optical telescopes are the alternative solution for this function. Under a \$189 million contract, Boeing has overall responsibility for the SBSS system, including the ground system and initial mission operations and including Ball Aerospace which is providing the satellite and sensor. The 1 t satellite has a sensor sensitive to visible wavelengths with a large aperture that provides a wide field of view. The sensor is mounted on a two-axis gimbal so that it can be quickly and efficiently moved between targets. It has twice the sensitivity and triple the probability of detecting threats of alternative techniques such as the MSX Space-Based Visible Sensor (SBV), which ceased operation in December 2008, and can monitor objects as small as a 1-meter cube all the way out to the geosynchronous belt. The SBSS satellite is in a 390-mile high circular sun-synchronous orbit (inclination 97.8°). It is operated from the Satellite Operations Center located at Schriever AFB, Colorado Springs. Initial operational capability was delayed until August 2012 due to faulty electronics which reset when passing through the South Atlantic Anomaly (a low hanging spur of the ionosphere) requiring a software upload in April 2012.

The 113 kg ORS-5 satellite was launched in August 2017 to act as a bridge between the SBSS satellite and the yet to be confirmed SBSS follow-on program. Also referred to as SensorSat, ORS-5 is in an equatorial orbit at 600 km altitude. The onboard sensor is a CCD imager that provides continuous imaging of the geosynchronous belt. The primary ground station is at the Air Force Satellite Control Network facility in Guam, with backup in Diego Garcia plus limited backup in Hawaii. Prime contractor for the \$87 million development contract was the Massachusetts Institute of Technology's (MIT) Lincoln Laboratory. The Northrop Grumman (Orbital ATK at the time) Minotaur-IV launcher costs \$24 million. What is now the Space Rapid Capabilities Office at the Kirtland Air Force Base managed the program. In orbit the satellite is operated by the Air Force Space Command's 50th Space Wing at Schriever AFB.

The USAF is reviewing the requirements for follow-on satellites that would make up a constellation in space taking into account the results from the SBSS-1 and ORS-

5 satellites and from improvements in ground-based technology such as the \$110 million Space Surveillance Telescope at White Sands Missile Range, New Mexico. The SBSS follow-on is intended to continue the expansion of data collection of the geosynchronous belt and to complement the up close inspection capabilities of the GSSAP system (see section “GSSAP”).

## GSSAP

Four Geosynchronous Space Situational Awareness Program (GSSAP) satellites are in orbit. They are able to perform rendezvous and proximity maneuvers to allow close-up looks at spacecraft in geosynchronous orbits with their electro-optic sensors and can provide the location, orbit, and size of satellites and space objects. With a price tag thought to be about \$700 million, GSSAP operates in a “near-geosynchronous orbit regime” to provide accurate tracking and characterization of man-made orbiting objects (Fig. 12).

In 2015, Gen. John Hyten, the head of Air Force Space Command, said that the Defense Department had used the satellites to capture “truly eye-watering” images for unspecified users while they were in test mode. The system improves the US capability to rapidly detect, warn, characterize, and attribute disturbances to space systems in the geosynchronous environment. One unclassified use of the system was to check on the MUOS-5 communications satellite (see section “MUOS and UFO”) that ran into propulsion problems about halfway to geosynchronous orbit.

The satellites were built by Northrop Grumman (formerly Orbital ATK) of Dulles, Virginia. The first two were launched in July 2014, and the program achieved initial operational capability in September 2015. Two replenishment satellites were launched in August 2016 and accepted into operation in September 2017. The Air

**Fig. 12** MiTEx mission badge



Force ordered two more GSSAP satellites from Northrop Grumman for an undisclosed price in late 2016.

Operated by the Space & Missile Systems Center at Los Angeles AFB during its in-orbit test phase, GSSAP was turned over to 1st Space Operations Squadron of the 50th Space Wing of the 14th Air Force at Schriever AFB in Colorado CO for the operational phase.

GSSAP is one element of the US infrastructure aimed at addressing Space Situational Awareness. The other main elements are on ground – a worldwide network of radars and telescopes that provide the main inputs to a detailed catalogue of space-based objects. A recent upgrade to that ground infrastructure called the Space Fence is scheduled to begin operation in 2019. In June 2014 Lockheed Martin won the \$914 million contract to build the Space Fence, an S-band phased array radar that the Air Force says will improve its ability to detect and track Earth orbiting objects. Defense Department officials said they are optimistic that on the best days, the Space Fence may be able to track objects as small as 1 cm. That's a marked improvement over the current network of radars and sensors, which tracks objects 10 cm and larger. That additional precision means the Air Force will have tracking data for 200,000 objects, up from the approximately 20,000 objects it tracks today. In turn, the new data could lead to an orders of magnitude increase in collision warnings.

The initial Space Fence facility on Kwajalein Island in the west-central Pacific Ocean will deliver 80 percent of the envisioned overall capability. After that enters operation, work is planned to start on a second site in Western Australia which would become operational around 2022 and improve the timeliness and accuracy of observations.

Two MiTeX satellites launched in 2006 were precursors to GSSAP, demonstrating a new way to monitor objects in geostationary orbit – go there and look around. The 225 kg satellites are small and thus difficult to detect from the ground. Their ability to inspect geostationary orbiting objects was demonstrated in December 2008 and January 2009 when they were commanded to approach the malfunctioning 2½ ton DSP-23 early warning satellite (see section “[Missile Early Warning Satellites](#)”) that was drifting eastward across the geostationary arc at about 1° per week from its 8.5°E longitude starting point – posing a threat to other satellites as it drifted. The MiTeX microsattellites tested a range of technologies for the Defense Advanced Research Projects Agency (DARPA), the US Air Force, and the US Navy. These include avionics, advanced communications, fuels that spontaneously ignite on contact, solar cells, and new software. One was built by Northrop Grumman (Orbital Sciences at the time), and the other was by Lockheed Martin.

## Research Satellites

US military technology proving and mission demonstration satellites are typically the subject of two or three launches each year. The satellites are often members of a series with names such as TacSat, Operationally Responsive Space (ORS), STPSat,

FalconSat, etc. Increasingly, CubeSats and other forms of micro- and nano-satellites are part of the mix. Given their ad hoc and nonoperational nature, they will not be described here – with the following exception.

The most widely reported USAF research space mission in recent years has been that of the X-37B series so that will now be briefly described. The X-37 began as a NASA project in 1999, before being transferred to the Department of Defense in 2004.

Two X-37B robotic spaceplanes (mini, unmanned versions of the space shuttle) have been into orbit and reentered successfully and then landed horizontally and autonomously. The schedule of the flights of Orbital Test Vehicle (OTV) -1 and OTV-2 is shown in Table 1. Each vehicle weighs about 5 t (barely one-twentieth that of the space shuttle), and they have been launched from Cape Canaveral, Florida, on an Atlas V 501 or Falcon 9 rocket and landed at Vandenberg Air Force Base, California, or at Kennedy Space Center. Their orbits have not been publicly announced, but amateur enthusiasts have documented variations of orbit during each flight, generally in the 300–400 km altitude region with an inclination of about 40°. For example, OTV-2 was in a  $330 \times 340 \text{ km} \times 42.8^\circ$  orbit until a series of burns lowered it to 280 km 3 weeks before its reentry.

X-37B program manager Lt. Col. Tom McIntyre noted that “with the retirement of the space shuttle fleet, the X-37B OTV program brings a singular capability to space technology development. The return capability allows the Air Force to test new technologies without the same risk commitment faced by other programs.”

The details of the X-37B’s mission are classified, as is its payload. The US Air Force’s deputy undersecretary for space programs, Richard McKinney, described it in 2010 as “a test vehicle to prove the materials and capabilities, to put experiments in space and bring them back and check out the technologies. This is, pure and simple, a test vehicle so we can prove technologies and capabilities.”

The X-37B project is managed by the USAF’s Rapid Capabilities Office located at Joint Base Anacostia-Bolling in Washington, DC, with mission control for orbital flights based at the 3rd Space Experimentation Squadron at Schriever Air Force Base in Colorado. The vehicle was developed by Air Force Research Laboratory offices AFRL/RV at Kirtland AFB, New Mexico, and AFRL/RB (Air Vehicles) at Wright-

**Table 1** OTV flight schedules

	Flight 1	Flight 2	Flight 3	Flight 4	Flight 5
<b>Vehicle</b>	OTV-1	OTV-2	OTV-1	OTV-2?	OTV-1?
<b>Launcher</b>	Atlas V 501	Atlas V 501	Atlas V 501	Atlas V 501	Falcon 9
<b>Launch</b>	April 22, 2010	March 5, 2011	Dec. 11, 2012	May 20, 2015	Sept. 7, 2017
<b>Landing</b>	Dec. 3, 2010	June 16, 2012	Oct. 17, 2014	May 7, 2017	TBD
<b>Landing site</b>	Vandenberg AFB	Vandenberg AFB	Vandenberg AFB	Kennedy Space Center	TBD
<b>Mission length</b>	224 days	469 days	674 days	717 days	>500 days



Patterson AFB, Ohio, with Boeing Phantom Works. This sets it apart from other USAF space projects which are mostly managed out of Los Angeles and indicates a closer connection with the “air” side of the Air Force.

---

## Future Prospects

The short-term upgrades and replacements for the various satellites described in this chapter have been covered alongside the description of the current systems. There are some general trends across all of the programs including:

- There is an increased, but still not universal, willingness within the US military and intelligence communities to use commercial satellite services.
  - In telecommunications, the military is a major purchaser of ad hoc commercial services but has avoided the long-term relationships with commercial suppliers of the type adopted in, for example, the UK and Spain.
  - In the surveillance world, the US military dominates the world marketplace for optical imagery. Recognizing its ability to influence the commercial market, it has underpinned the financing of the combined DigitalGlobe/GeoEye company, by entering long-term data and service purchase agreements with it. In parallel, it continues to build and operate very sophisticated systems itself without any sign of a letup.
  - The GPS navigation system remains a DOD program despite the fact that the service is the mainstay of an enormous global commercial business. With the entry of Russian, Chinese, and European systems with performance similar to GPS, and all providing the navigation signal free of charge, DOD will almost certainly have to continue funding the system.
- DOD space systems have with rare exceptions been late and over-budget. Many new systems in telecommunications and surveillance have been cancelled in recent years because of this, some of which have been mentioned in the previous sections.
  - The NRO Director from 2009 to 2012, General (Ret.) Bruce Carlson, worked wonders in overseeing the successful deployment of several much-delayed and much-needed surveillance systems in 2010–2012. It remains to be seen if NRO can continue this successful record after his departure.
  - Systems such as MUOS (Section “[MUOS and UFO](#)”) and SBIRS (Section “[Missile Early Warning Satellites](#)”) have been placed in orbit despite the fact that their support systems will not be fully available for some years to come. GPS-III (Section “[Global Positioning System \(GPS\)](#)”) is likely to follow suit.
- There is some recognition in the US military that large sophisticated satellites are sitting ducks for anti-satellite weapons and that more and simpler satellites might provide a more robust service. However, this intellectual analysis has largely failed to influence the latest US military space systems, which are generally larger than the previous generation. This situation is broadly at odds with the trend in the commercial space marketplace where small satellites have established an

---

important niche for customers willing to seek a compromise of price versus performance versus schedule.

- For the USA, “interoperability” usually means that the partners have to be compatible with US systems and often are required to purchase US equipment. The dominance of US forces in NATO means that this tendency is likely to continue.

---

## Conclusions

The US military space program continues to dwarf (a) the military space programs of all other countries combined and (b) of US civilian agencies such as NASA. The USA is unique in deploying military satellites of all types and on a global basis, and there is little sign that this will change in the next decade.

---

## References

- Anon (2009) AU-18 space primer. Air University Press, Maxwell Air Force Base, Alabama  
Norris P (2010) Watching earth from space. Springer Praxis, London/New York  
Richelson JT (2008) The US intelligence community, 5th edn. Westview Press, Boulder



Elina Morozova

## Contents

Introduction .....	1172
Main Launch Vehicles .....	1172
Angara Launch Vehicle Family .....	1174
Proton-M .....	1175
Soyuz-2 Launch Vehicle Family .....	1175
Soyuz-FG .....	1176
Strela .....	1177
Rockot .....	1178
Dnepr .....	1180
Operating Cosmodromes .....	1180
Baikonur Cosmodrome: Kazakhstan .....	1181
Plesetsk Cosmodrome .....	1182
From Svobodny to Vostochny Cosmodrome .....	1183
Kapustin Yar .....	1184
Yasnyy Cosmodrome .....	1185
Guiana Space Centre .....	1185
Sea Launch .....	1186
Conclusions .....	1187
References .....	1189

## Abstract

This chapter provides an overview of the current status of the Russian space launch program, including its main launch vehicle families and operational cosmodromes. A historical background, in particular on the achievements of the Soviet age and

---

E. Morozova (✉)

International Legal Service, Intersputnik International Organization of Space Communications,  
Moscow, Russian Federation

International Institute of Space Law (IISL), Paris, France

e-mail: [morozova@intersputnik.com](mailto:morozova@intersputnik.com)

their application in the post-Soviet times, is given, and future developments are described, including those which are guided by government policy in the field of space activities, the federal space program, and specific dedicated projects, which are adopted to secure efficient implementation of the relevant tasks (see Federal Dedicated Program. Development of Spaceports to Support Space Activities, 2017–2025 (approved by the Government of the Russian Federation on 13 Sept 2017) and Federal Space Program of Russia for 2016–2025 (approved by the Government of the Russian Federation on 23 March 2016).

---

## Introduction

In early October 1957, the world's first artificial Earth satellite launched into orbit by the Soviet R-7 rocket opened the way to outer space. A few pioneering accomplishments in the exploration and use of outer space achieved by the USSR followed shortly. They include the first space object that reached another celestial body and hard-landed on the Moon, the first human spaceflight and the first woman in space and the first spacewalk and the first docking and crew exchange between two manned spacecraft.

In the ensuing long-term space race of the USSR and the USA, considerable progress was made in space industry, including the development of launch vehicles of various classes and the construction of space launch facilities. Today, Russia, the USSR's successor since the very end of 1991, is sometimes called a "space carrier." Indeed, the existing fleet of space rockets helps to solve complex tasks of delivering all types of payloads to different Earth orbits. More so, in particular launch areas such as the delivery of crews to the International Space Station, Russian technology enjoys a monopoly.

During the entire history of post-Soviet space activities from 1992 to 2018, Russia remained the world leader in terms of the number of annual launches most often for a total of 19 years, 6 years second to the USA (1996–1999, 2003, and 2017), and 2 years second to the USA and China (2016 and 2018). For 13 years where the largest number of launches took place (1992–1995, 2000–2002, 2005–2006, and 2008–2010), Russia nipped and tuckered or even outpaced the USA and China combined. In 2019, Russia is planning to carry out about 45 launches and regain the lead (Opening remarks by Dmitry Medvedev 2019). Along with that, one of the priority tasks remains to commercialize Russia's space industry and increase its share in the international market of launch services (Briefing by Yuri Borisov 2019).

Russia has all the trumps in hand to accomplish this task.

---

## Main Launch Vehicles

The R-7 Intercontinental Ballistic Missile (ICBM), used for the first time as a carrier of space objects, was named Sputnik. Having made two successful launches only, it was sent for further modernization. Sputnik-1, the first artificial satellite, weighed

just about 80 kilograms, while it was required to put much heavier payloads into various Earth orbits. The mass of the third artificial satellite exceeded 1.3 tons, a convincing indication that significant progress could be made in improving launchers' characteristics within a very short period of time.

Indeed, the 1960s competition between the Soviet Union and the USA to be the first on the Moon made them contend at the limit of scientific and technical capabilities. The USSR developed the Luna and the Molniya launch vehicles, which succeeded in performing the first hard and the first soft landings on the Moon of the Luna-2 and Luna-9 missions in 1959 and 1966, respectively. The Molniya was also successful in launching automatic interplanetary stations to another nearest planets of the solar system – Venus in 1961 and Mars in 1962. In 1963–1964, the Polyot launching vehicle flew Soviet maneuvering satellites.

On April 12, 1961, the first ever cosmonaut of the planet, Yuri Gagarin, was successfully launched on the Soviet Vostok rocket carrier. In order to provide the ability of launching manned space vehicles of a greater mass, the Vostok vehicle had to be modified. In turn, the Voskhod was capable of launching manned spacecraft with a crew of two or three people. Further modernization of the Voskhod, which was named Soyuz, made it possible to launch new manned spacecraft with the same name, Soyuz, capable of maneuvering and docking in orbit. Subsequently, the Soyuz was repeatedly refined and improved and significantly expanded the launch capabilities of the USSR and later of Russia.

Then the two spacefaring rivals were challenged to try strength against each other in the superheavy class to send a human to the Moon. In 1960, the development of Soviet high-power launch vehicles began, and the project was named N1-L3. In 1964, the USSR Government decree stated, for the first time, that the most important challenge to be met in space exploration by the N1 launch vehicle was to explore the Moon including an expedition landing on its surface and its subsequent return to the Earth. Besides the vehicle itself, the complex included a lunar system called L3 intended for the launching to the Moon and returning back to the Earth of a crew of two people with only one of them to be actually put down on the lunar surface. Four trial launches of the N1 were in varying degrees a failure. Just before the fifth one, after a considerable modification, the program was shut down in 1974. The most extensive experience gained in designing and manufacturing the N1 was later employed in the development of the Energia heavy-lift launch vehicle capable of injecting payloads of up to 100 tons as part of the Energia-Buran reusable space system. The first and the second successful launches in 1987 and 1988 proved that the Energia was a unique achievement of the world's rocket building industry with no analogues. However, a total recession in space industry coinciding in time with the collapse of the USSR had an unfavorable effect on the Energia-Buran project. In 1992, all the works were terminated.

In the Soviet epoqe, hundreds of ministries and thousands of organizations were involved in the creation of launch vehicles of various classes and types, and the largest scientific and production centers were located not only in Russia but also in Ukraine which is famous for its Cyclone and Zenit launch vehicles, Belarus, and other USSR republics. A number of successful developments of that age continue to

be successfully employed in post-Soviet countries, while Russia itself is currently using quite a few launch vehicle families.

## **Angara Launch Vehicle Family**

Angara is the youngest family of Russian launch vehicles, a large part of which is still being developed and tested. Its commissioning is considered a national task of special importance as it will allow Russia to launch all types of spacecraft from its own territory and, thus, ensure its independent-guaranteed access to outer space.

A production order for Angara was placed by Roscosmos State Corporation and the Ministry of Defence of the Russian Federation meaning that the new launch vehicles are expected to satisfy the whole range of domestic needs, including civil, scientific, and military. The Angara space rocket complex uses exclusively domestic hardware elements by Khrunichev State Research and Production Space Center, one of the core companies in Russia's space industry, in cooperation with other Russian industrial and construction entities.

Another distinctive feature of the new complex is that the Angara launch vehicles are environmentally friendly. They do not use aggressive and toxic heptyl-based rocket fuels. This can significantly improve the environmental safety of the complex both in the regions adjacent to launch sites and in areas where spent stages land.

The Angara family includes launch vehicles of various classes. The basis for the development of the different classes is oxygen-kerosene all-purpose space rocket modules, the total number of which in the first stage determines the carrying capacity of the launch vehicle. The modules of the first and second stages are equipped with the liquid jet engine RD-191, the upper stages' modules – with the RD-0124A engine. When the design and construction stage is completed, Angara will provide a full range of lift services – light, medium, and heavy, putting up to 37.5 tons of payload into low Earth orbits (For a launch to the low reference Earth orbit by the Angara-A5V modification.). The development of a heavy modification for manned spacecraft launches, the Angara-5P, is also being discussed.

Unique technical solutions and extensive use of unification allow the whole Angara family to be launched from a single site. The ground infrastructure of the Russian Plesetsk Cosmodrome is able to provide launches of Angara light, medium, and heavy launch vehicles. The second launch complex is planned to be built at the new Cosmodrome Vostochny (The Angara created for launches from the Vostochny Cosmodrome is also called the Amur.).

The prototype of the first stage of the light Angara-1.2 launch vehicle passed flight tests three times – in 2009, 2010, and 2013 – as part of the first Korea Space Launch Vehicle (KSLV-1). A contract for KSLV-1 had been signed by Khrunichev Space Center in 2004. Flight testing of the Angara space rocket complex at Plesetsk began in 2014 – first, of the light-class rocket Angara-1.2.PP and, then, of the heavy-class Angara-A5.1L. Each performed one successful launch. The next flight of the heavy Angara-5 is scheduled for 2019, and in 2020 the whole scope of works on its development and manufacture is to be commissioned.

## Proton-M

The Proton-series launch vehicles, with more than 400 launches behind, are well known around the globe and enjoy a high commercial potential on the world market. They are the basis of the Russian space transport system as well, being frequently used under various Russian state and commercial programs. Khrunichev State Research and Production Space Center is the vehicle's designer and manufacturer.

The currently utilized Proton-M is the advancement of the Proton-K launch vehicle with improved energy and mass, operational and ecological characteristics, and reliability. A new control system based on an onboard digital computing complex has been installed on the upgraded Proton-M. It helps burn up all fuel, thus improving the energy characteristics and environmental performance of the launch vehicle, and in spatial maneuvering during the active part of the vehicle's flight, thus extending the range of possible inclinations of the reference orbits; simplifies onboard electronic systems; and promptly assigns and changes a flight task. Proton-M has also received a lighter and a more voluminous head fairing which significantly increases space for payload accommodation, including the accommodation of several payloads of various types for carrying out group launches.

Proton-M is a heavy-class launch vehicle consisting of three stages with RD-series engines – the RD-276 in the first stage, RD-0210 and RD-0211 in the second stage, and RD-0213 and RD-0214 in the third stage. The first Proton-M launch with the Breeze-M upper stage took place in 2001. Today, such launches can inject payloads weighing more than 6 tons into geosynchronous transfer orbit or up to 3.3 tons directly into geostationary orbit. The Proton launch complex at Baikonur Cosmodrome consists of two launch sites united by a shared communications network and servicing facilities and operated autonomously. Kazakhstan's permission to fly the Proton-M from Baikonur is valid till 2025.

In 2021–2022, Proton-M can be replaced with the new Angara or the new Soyuz-5 launch vehicle. Both variants have been discussed; however, the most recent public announcements favor Angara (Telesputnik 2019). A while ago, there was discussed the Proton-Medium, a light version of the Proton-M without its third stage. An agreement of intent on the delivery of ten Proton-Medium was signed with OneWeb; however, no solid contracts were reached. It was therefore decided to offer OneWeb ten Proton-M in the existing version at the cost of a lighter Proton-Medium. Such a substantial discount would be beneficial to Khrunichev Space Center as well, as it did not need to invest heavily in the refurbishment of the launch pad for the sake of ten launches. With no economic grounds and a confirmed demand, there is no reason to expect that the Proton-Medium will be discussed again.

## Soyuz-2 Launch Vehicle Family

Soyuz-2 is a new-generation launch vehicle with significantly improved technical and operational parameters, developed by Progress Rocket Space Center, a Russian

joint stock company, on the basis of the legendary Soyuz-U which completed almost 800 launches in 1973–2017.

The launch vehicle was upgraded in two phases. During phase 1A, control and propulsion systems of the first and second stages were improved, and the Soyuz-2-1a modification was thereby provided with an enhanced injection accuracy and an increased payload mass for launches to low Earth orbits. During phase 1B, the launch vehicle's third stage was equipped with a modern engine, which further improved the energy capabilities of the Soyuz-2-1b modification. Both modifications consume environmentally friendly fuel components – kerosene and liquid oxygen.

Due to the growing demand for launches of small satellites, further rework of the Soyuz-2-1b modification was done. As a result of an additional modernization phase, phase 1 V, the two-stage light-class Soyuz-2.1v vehicle was developed, which can dramatically reduce manufacturing, launch, and operational costs for spacecraft in low circular and elliptical Earth orbits. After the flight design tests are completed, Soyuz-2.1v will expand the capabilities of the Soyuz-2 launch vehicle family.

Russia's Soyuz-2-1a, Soyuz-2-1b, and Soyuz-2.1v launches are carried out from Baikonur, Plesetsk, and Vostochny cosmodromes. For launches from the Guiana Space Centre which is a French and European spaceport to the northwest of Kourou in French Guiana, there were designed the Soyuz-ST-A and the Soyuz-ST-B modifications of the Soyuz-2 launch vehicle. For that purpose, the Soyuz-ST-series was adapted to the Guiana Space Centre specific requirements in terms of security as to receive the flight termination telecommand from the Earth, fitted with transmitters operating in the ultrahigh frequency band with a European frame structure telemetry, and adjusted to a higher level of humidity and a prior shipment by sea. The launch vehicles are equipped with a head fairing of the ST-type that meets international requirements and makes it possible to deliver the widest range of payloads into orbit.

The Soyuz-ST-A and the Soyuz-ST-B launches from the Kourou spaceport in French Guiana are serviced by Arianespace. Both modifications have been successfully launched since 2011, including for the European Galileo project. At the end of February 2019, Soyuz-ST-B launched the first six satellites of the low-orbit group OneWeb.

## **Soyuz-FG**

Soyuz-FG is another Russian launch vehicle developed on the basis of Soyuz-U and built by Progress Rocket Space Center. It is a middle-class three-stage launch vehicle using environmentally friendly kerosene and liquid oxygen as fuel. In order to increase the specific impulse of propulsion systems and the load capacity of the vehicle, upgraded engines with new nozzle heads are used in the blocks of the first and second stages. (The Soyuz launch vehicle modification FG was named after the English transliteration of “ФГ” in Russian, which stands for “форсуночные головки” translated as “nozzle heads.”)



It is designed to launch into near-Earth orbit automatic spacecraft for socioeconomic, research, and special purposes, as well as Soyuz-type manned spacecraft and Progress-type cargo spacecraft under the International Space Station (ISS) project. Since 2011, after the completion of the US Space Shuttle program, Soyuz-FG has been the world's only means of delivering crews to the ISS. (The situation may change in the second half of 2019, when SpaceX's Crew Dragon can start to carry astronauts to and from ISS. SpaceX successfully launched its first Crew Dragon capsule to ISS in March 2019. The Demo-1 flight was uncrewed, however proved its operability. Sierra Nevada Corporation is also working on a reusable multi-mission space utility vehicle Dream Chaser which is awaiting its first flight in 2021.) Soyuz-FG is capable of launching up to 7.2 tons of payload with a manned space mission, while the payload weight of a cargo mission amounts to 7.4 tons.

With the confirmed indicator of operational reliability of 0.985 (Progress Rocket Space Center 2014–2018), Soyuz-FG is one of the safest launch vehicles in the world. The only failure happened in October 2018 is when a Soyuz-FG rocket carrying a Soyuz MS-10 spacecraft with a crew on board crashed due to the abnormal separation of one of the side blocks, which hit the central block near the fuel tank with the bow, what led to its depressurization and, as a result, to the loss of stabilization of the launch vehicle. Russian cosmonaut Alexey Ovchinin and NASA astronaut Nick Hague, who were onboard Soyuz MS-10, were not injured, and their landing was secured by an emergency rescue system. Both crew members accompanied by Christina Koch of NASA arrived safely at ISS on March 2019, following a successful Soyuz-FG launch and docking of their Soyuz MS-12 spacecraft.

Soyuz-FG is also used for commercial and scientific launches, among them the launch in 2003 of the first planetary mission currently being conducted by the European Space Agency (ESA) for the study of the Red Planet titled Mars Express and the launch in 2005 of the first Venus exploration mission of ESA named Venus Express.

All Soyuz-FG launches are performed from the Baikonur Cosmodrome, which is the only spaceport with a Soyuz-FG launch site. In 2020, the use of Soyuz-FG is planned to be ceased as the existing stock of the Soyuz-FG rockets is going to be exhausted by the end of 2019. Manned launches will be transferred to Soyuz-2.1a. An order for the first three launch vehicles of the new type has already been placed with Progress Rocket Space Centre, and the first launch is scheduled for spring 2020.

## **Strela**

In 1980, the silo-based ICBM RS-18 (SS-19 modification 2 Stiletto under the NATO classification), which had been developed by the Soviet Central Design Office of Machine Building, was accepted for service. Capable of carrying up to 6 warheads, it was the most numerous strategic weapons in the Soviet nuclear fleet with a launch heritage of over 150 flights. A total of 360 missiles were placed on high alert. The mass production of the missile by the Moscow Khruichev Machine-Building Plant

stopped in 1985. With 35 years' service time, it is going to meet its end of life in 2020, unless extended.

In accordance with the 1993 Strategic Arms Reduction Treaty, a bilateral agreement between Russia and the USA on the reduction and limitation of strategic offensive arms also known as START II, the Russian strategic nuclear forces had to remain armed with not more than 105 RS-18, converted into single-block missiles. There arose the question of how to reduce the arsenal of these missiles. One of the options was to convert them to launch vehicles and use them for commercial launches.

Thus the RS-18 missile became the basis for the Strela and the Rockot launch vehicles, developed respectively by NPO Mashinostroyeniya, the successor to the developer currently known as Joint Stock Company Military Industrial Corporation NPO Mashinostroyeniya, and Khrunichev State Research and Production Space Center, the successor to the batch production plant manufacturer.

The Strela is a more recent conversion version of the decommissioned Russian ICBM. Unlike the Rockot, it requires only minor modifications to the original missile. It is a liquid-propellant two-stage light-class launch vehicle made according to a tandem scheme. The Strela launch vehicle can be equipped with one of two types of space head parts, which differ in fairings and, as a consequence, in the size of the payload placement space. The use of a specific type of space head depends on the features of the payload. It is capable of launching payloads of up to 2 tons in near-Earth orbits or in the upper atmosphere of the Earth.

The Strela's launches are carried out from the Baikonur Cosmodrome. The launch vehicle is located in a transport and launch container; the launch is carried out from a launch silo. Only three launches were performed in 2003, 2013, and 2014 each, all being successful. Besides the first test run, the Strela launched two Condor-series remote sensing satellites developed by NPO Mashinostroyeniya, the latter launched in the interests of a foreign customer (NPO Mashinostroyeniya 2019).

## **Rockot**

As well as the Strela, the Rockot was also developed based on stocks of the decommissioned Russian RS-18 ICBM, however, by another space industry entity – Khrunichev State Research and Production Space Center. The first Rockot test suborbital launches were performed in 1990 and 1991 from the Baikonur Cosmodrome. The first demonstration commercial space launch took place in 2000.

The Rockot is a light-class launch vehicle designed for launching small- and medium-size spacecraft of up to 1.95 tons into low Earth orbits (Khrunichev Space Center 2019). It is particularly suitable for launches into Sun-synchronous, near polar, and highly inclined orbits. The Rockot's head fairing allows placement of one or more spacecraft and is, therefore, suitable for co-launches.

The vehicle is made according to a three-stage scheme with a sequential arrangement of stages. (This is the main difference from the Strela launch vehicle which is a

later version of the RS-18 ICBM conversion with a minimized change in the design of the rocket and the launch complex.) The first two are the booster stack of the converted missile, and the third is the Breeze-KM upper stage. High-efficiency liquid rocket engines operate on nitrogen tetroxide and asymmetric dimethyl hydrazine. Experts from Khrunichev Space Center worked hard to ensure the environmental safety of launches, including the selection of routes of injection and the arrangement of the spare stages landing fields.

The Rockot's high performance largely stems from the use of the Breeze-KM upper stage, which provides a wide range of options for spacecraft injection into orbits. The upper stage equipment is capable of controlling the attitude of the spacecraft with high accuracy, as well as providing its power supply during the launch and during the orbital flight for up to 7 hours. The ability to repeatedly, up to eight times (Roscosmos State Corporation 2019a), turn on the propulsion system of the upper stage makes complex co-launches possible. A special transition system allows the spacecraft to be separated from the upper stage with minimal disturbances.

Both state and commercial Rockot launches are performed from dedicated launch facilities, a transport and launch container, at the Plesetsk Cosmodrome, which is currently the only "home" spaceport for the Rockot. Five silo launchers for the RS-18 ICBM were earlier available at the Svobodny Cosmodrome; however no launches of Rockot vehicles have been carried out from that facility till its closure in 2007 (Lenta.ru 2007).

In 2000–2018, Rockot performed 29 single, dual, and multiple payload launches, 25 of which were fully successful. The most recent mission occurred in November 2018, when three Strela-3 M communications satellites for the Russian Ministry of Defence were launched, bringing the number of government payload launches to 15. Fourteen missions were purely commercial, with the latest launch of the Sentinel-3B remote sensing satellite in April 2018. The Sentinel-3 mission is jointly operated by ESA and EUMETSAT to deliver operational ocean and land observation services to support ocean forecasting systems, environmental monitoring, and climate monitoring.

Commercial launches are operated by Eurockot Launch Services GmbH, the Bremen, Germany, based joint venture of ArianeGroup and Khrunichev Space Center, which invested financially in the development of modern satellite preparation and launch facilities dedicated to the Rockot at the Plesetsk Cosmodrome.

In February 2015, the Ukrainian government banned the supply of components for the Rockot launch vehicle to be used for Russia's military space missions; however, it did not withdraw from their shipment for civil space programs (Lenta.ru 2015). In March 2018, Khrunichev Space Center reported that, in order to ensure import substitution and full Russian production management, the design documentation was being worked out in order to give a second wind to the Rockot 2 vehicle (Zvezda 2018). In addition, in 2020, the lifetime of the RS-18 ICBM produced before 1985 will expire. In this regard, the Russian Ministry of Defence intends to abandon the conversion of Rockot systems, replacing them with the Russian Angara.

## Dnepr

Dnepr is another example of a converted launch vehicle developed on the basis of ICBM technology. The RS-20 (SS-18 Satan under the NATO classification), one of the heaviest missiles (Roscosmos State Corporation 2019b), was developed in Soviet times by the Yuzhnoye Design Office based in Dnepropetrovsk, Ukraine, and remained in operational service for at least 15 years (RS-20 service life was subsequently extended.). When the period of its operation came to an end, it was decided to use the carrier of the nuclear warhead in the conversion program called Dnepr, that is, to adapt the rocket for peaceful space launches. This decision was preceded by scientific research and preliminary design efforts, which confirmed that minimum modifications would guarantee a cost-effective solution. First, there is no need to scrap the system. Secondly, the missile performs an important peaceful mission. Finally, it helps the military to make sure that the RS-20 technology, despite an advanced age, is still reliable.

During 1992–2003, a team of Russian and Ukrainian companies together with the Russian Ministry of Defence were involved in developing a space launch system based on the RS-20 being withdrawn from service. International Space Company Kosmotras, a Russian joint stock company, was tasked to commercially operate this RS-20 ICBM-based space launch system.

The Dnepr is a liquid-fueled three-stage launch vehicle. The first and the second stages remain original with no modifications, while the third stage received an upgraded control system that implements the required flight program of all three stages. The launch vehicle is designed for rapid high-precision launches into near-Earth orbits with altitudes of 300–900 km of single or multi spacecraft weighing up to 3.7 tons. Environmental monitoring after the Dnepr launches confirms their complete safety for life and the environment. Environmentalists have never recorded a negative impact from the components of rocket fuel, its combustion products, or an excessive acoustic impact (Rossiyskaya Gazeta 2014).

The first commercial Dnepr mission lifted off in 1999. Over 20 years of operations, the launch vehicle has performed 22 launches, only 1 of which was a failure, thereby providing the mission reliability factor 0.97 (International Space Company Kosmotras 2019a), with a total of 128 payloads injected into Earth orbits in the interests of renowned universities, major space industry companies, and space agencies from France, Germany, Italy, Japan, Saudi Arabia, the UK, the USA, Thailand, South Korea, and other countries (International Space Company Kosmotras 2019b). Dnepr launches are currently performed from the Baikonur Cosmodrome and the Yasny launch base.

---

## Operating Cosmodromes

Guaranteed access to outer space is one of the cornerstones of Russia's state policy in the field of space activities and a significant factor influencing geopolitical interests of modern Russia. Today, it operates five cosmodromes – Baikonur, Plesetsk,

Vostochny, Kapustin Yar, and Yasny – and exports Russian launch vehicles abroad to be employed at the Guiana Space Centre. Baikonur, even though located in the territory of Kazakhstan, still remains the main spaceport of Russia; however, all future developments of the exploration and use of outer space are mainly associated with the newest and the first purely civil spaceport in Russia called Vostochny. After the purchase deal of Sea Launch by Russian S7 Group in 2016, a sixth Russian spaceport can be added, though not governmental but private.

## **Baikonur Cosmodrome: Kazakhstan**

The territory of Baikonur amounts to 6717 square kilometers. It is not only the largest, it is also the oldest spaceport in the world with a great history. The construction project was approved as long ago as 1955. Within an unusually short time, by 1957, there was erected a launch complex for the R-7 ICBM, the prototype of the modern Soyuz launch vehicle. In the same year, the first artificial Earth satellite, Sputnik-1, was launched from Baikonur, followed by the first ever spaceflight in the history of humankind performed by Yuri Gagarin in 1961 and the first spacecraft's launches to the Moon, Mars, and Venus. The cosmodrome performed almost 5000 space launches in total. Today, Baikonur remains the only spaceport that delivers manned spacecraft to the ISS. (See also the section on the Soyuz-FG which is the launch vehicle used for manned spacecraft missions.) Manned missions used to be carried from the John F. Kennedy Space Center in Florida, USA, until the NASA Space Shuttle program was closed in 2011; however, they can be resumed in the second half of 2019 by SpaceX's Crew Dragon followed by Sierra Nevada Corporation's Dream Chaser which is awaiting its first flight in 2021. Cargo spacecraft to the ISS are also launched from Baikonur.

After the dissolution of the USSR, Baikonur Cosmodrome found itself in a foreign state. It was therefore agreed that Baikonur Cosmodrome and the city of the same name, which make up the Baikonur complex, were rented by Russia from Kazakhstan. A contract between the Government of Kazakhstan and the Government of Russia was executed in 1994 (see the Rent Contract for the Baikonur Complex Between the Government of the Republic of Kazakhstan and the Government of the Russian Federation dated December 10, 1994, as later amended by the protocols on amendments of 2008, 2017, and 2018 (the latter two are still pending entry into force)) and provided for a 20-year rental term which could be extended, in the absence of objections, for another 10 years, meaning that the initial rent term might expire as soon as in 2024. In November 2018, a protocol on amendments to the contract was signed by both states to prolong the rent of the Baikonur complex till 2050. The protocol, and the extension itself, will come into force upon implementation by both parties of the necessary domestic procedures. The rental of the Baikonur complex costs Russia 115 million US dollars annually. The basic principles of Russia's use of Baikonur, including settling of international space law matters and the launching state issue in particular (see the Agreement between the Russian Federation and the Republic of Kazakhstan on the Basic Principles and Conditions

of the Use of the Baikonur Cosmodrome dated March 28, 1994.), are determined in a bilateral international agreement. (In the event of damage caused by the activities of Baikonur Cosmodrome in the course of Russian space programs, Russia is liable as a launching state in accordance with the Convention on International Liability for Damage Caused by Space Objects of March 29, 1972. In this case, Kazakhstan is not considered as a party to the joint launch or a launching state. In the case where the launch of a space object is carried out by Russia together with Kazakhstan, liability for damage is determined by Article V of the 1972 Liability Convention. In the event that the launch of a space object is carried out by Russia together with other states, these states shall be jointly and severally liable for any damage caused in accordance with the 1972 Liability Convention, and Kazakhstan is not considered as a participant in the joint launch or a launching state.)

In order to reduce its dependency on Baikonur, Russia has started to upgrade its own space facilities.

## **Plesetsk Cosmodrome**

The Plesetsk Cosmodrome is the one that has been upgraded and is currently the main government test cosmodrome of the Ministry of Defence of the Russian Federation. In mid-2001, the cosmodrome was included in the Russian Space Forces. It is also highly involved in Russian and international space programs related to scientific and commercial launches of unmanned spacecraft. Light-class Angara-1.2, Soyuz-2.1v, and Rockot, as well as middle-class Soyuz-2.1a and Soyuz-2.1b and heavy-class Angara-A5 launch vehicles, are operated at the Plesetsk Cosmodrome.

With a total area of 1762 square kilometers, Plesetsk is one of the world's largest spaceports. It is located in the Plesetsk district of the Arkhangelsk region in the Northwest of Russia and the northernmost location for a spaceport on the globe. Though the technical facilities of Plesetsk make it possible to launch various spacecraft into all types of orbits, including geostationary orbit, such a long distance from the Earth equator imposes certain limitations. (The linear speed of rotation of the Earth at the latitude of Plesetsk is 212 meters per second; at the latitude of Baikonur, 316 meters per second; and at the latitude of the Guiana Space Centre at Korou, French Guiana, 460 meters per second. Plesetsk is particularly convenient for launches of spacecraft into high inclination and polar orbits.)

However, the choice of the cosmodrome location was largely determined by the tactical and technical characteristics of the R-7 ICBM, as Plesetsk had been initially deployed as a military unit of missile regiments armed with the R-7. First, it was essential that the territories of potential adversaries were within missile range, and the need for special secrecy was also taken into account. Secondly, the possibility of conducting and controlling missile test launches to the Kura missile range located in the Kamchatka region was important.

The history of the Plesetsk Cosmodrome begins in 1957, with the USSR Government's decree on the creation of a military facility with the conventional name

Angara. Since the launch of the first spacecraft from Plesetsk in 1966, more than 1600 space launches have been performed and about 2100 spacecraft for various purposes have been put into Earth orbits. Since 1968, the cosmodrome has been involved in the implementation of international space programs. In April 1972, for the first time in the USSR, a small French spacecraft, MAS-1, was launched from Plesetsk. In 1970–1990, the Plesetsk Cosmodrome held the world leadership in the number of space launches (From 1957 to 1993, 1372 launches were carried out from Plesetsk, while Baikonur took the second place with a total of 917 launches for the same period.) and is historically one of the sites with the world's highest launch frequency.

### **From Svobodny to Vostochny Cosmodrome**

The question of deploying a new Russian cosmodrome was raised before the leadership of the Russian Ministry of Defence in 1992. The main reason was that as a result of the collapse of the USSR, Baikonur was geographically outside the territory of Russia. Though the launches of spacecraft by light and medium-class launch vehicles could be carried out from the Plesetsk Cosmodrome, the issue of launches of heavy-class launch vehicles was particularly acute. Heavy Proton launch complexes were only available at the Baikonur Cosmodrome.

To choose a location for the new cosmodrome, the map of Russia was analyzed. Despite the vast territory of the country, only southern regions of Russia's Far East and Sakhalin Island were considered potentially suitable, and no places closer to the European part of Russia were appropriate for the placement of the cosmodrome. A significant distance from the main capacities of the Russian space industry was a great disadvantage. More so, Sakhalin Island turned out to be one of the most remote parts of Russia having no suitable railroad, resource, and production capacities. The final assessment of the several selected areas resulted in the choice of the district of the city of Svobodny in the Amur region as the location of the new Russian cosmodrome.

The history of the new Russian cosmodrome began in 1997. The Svobodny Cosmodrome, which can be translated into the English language as the Free Spaceport, is officially named the Second State Test Cosmodrome of the Ministry of Defence of the Russian Federation. During the whole time of its existence, only five space launches were performed by the Start 1.2 launch vehicle with the latest one in 2006. Four of them were made in the interests of foreign customers – the USA, Israel, and Sweden. According to some reports, in 2005, the Security Council of Russia decided to close the cosmodrome as part of the reduction of the armed forces due to the low intensity of launches and insufficient funding. In 2007, the closure of the cosmodrome was publicly announced, and since then it has not functioned.

Very soon, the question of a new Russian full-fledged multitask cosmodrome, as an alternative to Baikonur, was once again posed. The decree on the construction of the Vostochny Cosmodrome was signed by the President of Russia in 2007, and the

memorial sign was laid in honor of the start of works on the first Russian civil cosmodrome in 2010. There were some other tasks behind such a significant project – the cosmodrome was built not only to provide independent access to outer space, to guarantee the implementation of international and commercial space programs, to reduce the cost of the Baikonur Cosmodrome, but also to improve the socio-economic situation in the Amur region of Russia.

Vostochny means “Eastern” in the Russian language. Indeed, it occupies an area of about 700 square kilometers in the Far East of Russia, rather close to the Earth equator which makes launches from there more efficient, if compared with Plesetsk. The Far East area is underpopulated meaning that space safety is not a big issue for this location, and the trajectory of launch vehicles does not pass over the territories of foreign States. Vostochny is located 45 kilometers north of the Svobodny Cosmodrome which means the proximity of an already well-developed railway, highways, and airfields.

The construction of the launch complex for the light- and medium-lift launches, being the major part of the first construction stage, began in 2012 and was completed in 2016. Today, the Soyuz launch pad is fully operational, and three of four launches have been a success. By the end of 2018, the first stage was expected to be fully completed. According to Roscosmos State Corporation, which is tasked with the Vostochny construction, all the first stage works have been actually done in time, while some papers required for a formal acceptance are being close to finalization (Ria Novosti 2019).

The second construction stage involves the deployment of a launch pad suitable for heavy launches in 2019–2025. A backup complex should be built for the start of the heavy Angara, which already exists in Plesetsk. The first Angara-A5 launch is scheduled for 2023. The existing infrastructure of Vostochny technically allows for a transfer of the manned spacecraft program from Baikonur after minor modifications, which is also planned to be done in the coming years by launching a manned spacecraft, the Federation, in an unmanned version first and with a crew shortly afterward. Recently, the President of the Russian Federation gave instructions to deploy a launch complex for the superheavy class at Vostochny no later than 2023, which constitutes the third stage of construction (Briefing by Yuri Borisov 2019).

## **Kapustin Yar**

The Kapustin Yar missile range occupies an area of about 650 square kilometers in the Northwestern part of the Astrakhan region of Russia, near the border with Kazakhstan. Officially, it is named the Fourth State Central Multipurpose Firing Range of the Russian Federation (Declassified photos of the Kapustin Yar missile range are available on the web-site of the Ministry of Defence of the Russian Federation at <http://mil.ru/files/files/kapyar/photos/index.html>).

Kapustin Yar was deployed in 1946 as the test site for the first Soviet missile weapons, both ballistic and surface-to-air. In October 1947, the first ever launch of a Soviet ballistic missile was conducted from Kapustin Yar, which remained the only



place to test Soviet missiles till 1957. At the same time, the missile range was also used for the exploration of outer space.

In 1951, two dogs, Dezik and Tsygan, were launched and safely returned to the Earth being the first higher mammals in outer space. To deliver the animals to the near-Earth space, a liquid-fuel single-stage R-1-type rocket was used, which is one of the first Soviet geophysical missiles employed in scientific research and experimental works. The rocket rose to a height of about 101 km reaching the Karman Line. In a state of weightlessness, the dogs spent about 4 minutes. Fifteen minutes after the launch, the container with the dogs landed safely a few kilometers from the launch pad. The first flight of Dezik and Tsygan was a significant step forward in outer space exploration. Post-flight examinations showed no serious changes in the animals' physiological state and no harmful effects on their organisms. They perfectly suffered overloads and weightlessness. This gave confidence to Soviet researchers in their plans to launch a human to outer space, what actually happened 10 years later.

In March 1962, with the launch of the Cosmos-1 satellite, Kapustin Yar became a cosmodrome. In 1969, the Intercosmos-1 satellite manufactured by a group of socialist countries took place, and this made Kapustin Yar open for international cooperation, which shortly continued with flying Indian and French satellites. Later it was mainly used for small research satellites' launches by the light-class Cosmos series launch vehicle. Today, Kapustin Yar serves as a site for launches of ballistic, geophysical, and meteorological missiles, as well as low-mass space objects.

## **Yasniy Cosmodrome**

Yasniy is the name of the fifth cosmodrome in Russia after Baikonur, Plesetsk, Vostochny, and Kapustin Yar. It is located in the Yasnenskaya district of Russia's Orenburg region and used for space launches on the Dnepr rocket. International Space Company Kosmotras, a Russian joint stock company, operates the cosmodrome and executes commercial contracts with customers. It orders and pays for launches carried out by the Ministry of Defence of the Russian Federation.

The first space launch from Yasniy dates back to mid-July 2006, when the US Genesis I satellite was launched into near-Earth orbit. A total of ten launches have been made so far, both single and multiple, of up to 33 space objects per launch, mainly for foreign customers. All launches were successful. The latest launch took place in 2015, when South Korea's KOMPSAT-3A remote sensing satellite was inserted into its target orbit.

## **Guiana Space Centre**

Russia and Kazakhstan, former USSR republics, are not the only countries which employ Russian launch vehicles' sites. The launch site of the Soyuz is also located at a distance of almost 10,000 kilometers from Russia – near the city of Korou in

French Guiana, an overseas department and region of France on the North Atlantic coast of South America.

The Guiana Space Centre is jointly utilized by the European Space Agency and the French National Centre for Space Studies (CNES). The spaceport became operational in April 1968. In 2003, the Russian-European project began when a decision was made at the government level to operate Soyuz launch vehicles at the Guiana Space Centre. A number of agreements, including intergovernmental (See the Agreement between the Government of the Russian Federation and the Government of the French Republic on Long-Term Cooperation in the Field of Development, Creation and Use of Rockets and the Placement of the Carrier Rocket Soyuz-ST at the Guiana Space Centre dated November 7, 2003.), were concluded, which laid the legal basis for signing contracts for the creation of the ground infrastructure of the Soyuz launch complex, the manufacture and shipment to French Guiana of the Soyuz-ST-series launch vehicles and the Fregat upper stages.

In May 2011, a ceremony was held to officially turn over the new launch complex to the European Space Agency and Arianespace, the operator of the spaceport. Two versions of the Soyuz launch vehicle, which was modified specifically for the Guiana Space Center, supplement the spaceport capabilities with medium-class launches. Soyuz entered service in October 2011 with an on-target maiden flight that orbited the first two European Galileo navigation satellites. Since then, two to three launches are carried out every year both in the interests of ESA and in the interests of commercial companies.

## Sea Launch

Sea Launch Company, an international consortium to develop and operate a sea-based space launch system, was established in 1995. The US Boeing; Russian S.P. Korolev Rocket and Space Corporation Energia; Norwegian ship-building enterprise Aker Solutions, previously known as Kvaerner; and Ukrainian space industry entities Yuzhnoye and Yuzhmash were the founders of this purely commercial international venture. By 1998, the buoyant complex in the equatorial waters of the Pacific Ocean near Christmas Island was constructed. The complex included a “home” seaport in Long Beach, California, a mobile sea-based launch platform named Odyssey and an assembly and command ship dubbed Sea Launch Commander. Such a unique location provided a significant increase in mass of the payloads to be launched due to the proximity to the equator, while the sea offered favorable conditions in terms of spacecraft’s delivery.

Sea Launch was tailored for the Zenit-3SL, a three-stage middle-class launch vehicle operating on environmentally friendly liquid oxygen and kerosene. It was based on the two-stage Zenit-2 launch vehicle developed by Yuzhnoye State Design Office, Ukraine, which performed 37 launches in 1985–2009 with the vast majority being successful. The Zenit-3SL is capable of putting payloads weighing more than

6 tons into medium and high Earth orbits, both circular and elliptical, as well as to geostationary transfer orbits.

Marketing research carried out during the implementation of the Sea Launch project revealed that it was advisable to carry out a number of launches of spacecraft weighing up to 4 tons not from the sea-based platform, but from the Zenit-M launch site of the Baikonur Cosmodrome. Such a diversification could also make the use of the available stock of the Zenit-series launch vehicles more efficient. An alternative commercial project was named Land Launch and opened another niche for Sea Launch Company.

The first commercial sea launch in 1999 was followed by another 35 launches, most of which were successful. However, in 2009, Sea Launch Company announced its bankruptcy, and the launch activity was suspended in 2014. According to some reports, losses could be caused by the fact that the company failed to ensure the planned intensity of launches: it was originally scheduled to carry out 2–3 consecutive launches in one exit to the launch pad (Kommersant 2010). Until 2016, negotiations were held on the sale of the project, as well as on measures to be taken to resolve financial and legal issues. In September 2016, Russian S7 Group became the owner of the Sea Launch complex. The launch activity was assigned to S7 Space, a dedicated branch of the group, which planned to resume launches at the very end of 2019 to be followed by another three launches in 2020 and four launches per year in 2021 and 2022.

In 2017, Yuzhmash, the Production Association Yuzhny Machine-Building Plant named after A.M. Makarov, announced the conclusion of a contract for the production and supply of 12 Zenit launch vehicles, but in March 2019, it became known that S7 Space canceled the order. The cancelation may be associated with the decision to replace the Ukrainian Zenit with the new Russian-made launch vehicles Soyuz-5 or Angara. Both alternative options were discussed; however, no final decision has been announced so far.

---

## Conclusions

Russia has successfully engaged in space activities for more than 60 years, having entered the space age as part of the Soviet Union and striding on as a separate state. On the one hand, after the dissolution of the USSR, Russia inherited the huge scientific and technical potential and technological developments of one of the two most powerful space nations of that time. But on the other hand, Russia was deprived of a large part of technologies and infrastructure put in place earlier. The launch vehicles that used to be Soviet became foreign, and the key launch site turned out to be located outside Russia's national territory. Also, it proved to be difficult for Russia to use remnants of its own technologies because suppliers of components had been scattered all over the enormous Soviet Union, and now Russia had to either import them or replace them with similar domestic parts. Political and economic turbulences during the late 1980s and the early 1990s dramatically affected Russia's space

activities and had a crucial negative influence on its space capabilities. A number of promising projects were abandoned. Many years have passed for new ones to come to life.

Nevertheless, Russia rightfully remains one of the leading space-faring nations and confidently occupies its well-deserved place among the world space industry leaders. Russian launchers rank among the best on the globe owing to their fine quality, high reliability, and cost-efficiency. Russia's capabilities are employed in launching scientific, civil, and military space missions, both domestic and in the interests of foreign partners. Russia remains open to international cooperation, including for sending crews and cargos to the ISS and for the purpose of deep space exploration and human space programs across the solar system. Ongoing technological advancement and capacity building is traditionally a key element of Russia's space strategy. The challenge ahead is to sustain, secure, and strengthen its position for the decades to come.

To keep Russia's guaranteed access to and presence in outer space, all major cosmodromes need to be retrofitted, upgraded, and kept functioning. In the first place, these are Vostochny, Plesetsk, and Baikonur that have to support federal programs and long-range dedicated tasks for the benefit of science and national economy as well as international and commercial space projects.

The main trend in the development of launch vehicle families in the period until 2025 is to reduce their lineup to two series based on the Soyuz and the Angara. The gamut of operating rocket carriers is also going to be reduced to six types to secure the whole variety of launches – light, medium, and heavy (Vzglyad 2016). Until 2030 there has to be developed a system with a superheavy booster capable of lifting no less than 50 tons, including for missions to the Moon, Mars, Jupiter, or other celestial bodies in the solar system (Main Provisions of the Principles of State Policy 2013).

The superheavy launch vehicle may be named Yenisei and will consist of flight-proven components – the first stage will be based on the first stage of the middle-class Soyuz-5, the second stage will get the famous Russian RD-180 engine that is exported to the USA, and the third stage will be borrowed from the heavy Angara-5 V (Lenta.ru 2019). The new Russian superheavy launch vehicle will use the heritage of the Soviet N1 and Energia. Thus, the Yenisei will be capable of carrying payloads of more than 100 tons to low-earth Earth orbits. The first vehicle is expected to be manufactured in 2027 with the first launch slated for 2028 from the Vostochny Cosmodrome. (This modification is also referred to as the Irtysh.) After 2030 it is planned to increase the lift capacity of the superheavy launcher to 130–180 tons and develop a reusable rocket system with a reusable first stage.

Today, the leadership in space industry remains of strategic importance. For Russia, this is not only a question of national defense and security or its position in the market of commercial launch services but also, and more importantly, a question of the status of Russia as a highly developed nation in terms of science and technology.

## References

- Briefing by Yuri Borisov, Deputy Prime Minister of Russia responsible for defence industrial complex, at the end of the meeting on the financial and economic condition of Roscosmos State Corporation and its subordinate organizations, 23 Jan 2019. <http://government.ru/news/35460/>. Accessed 29 March 2019
- Federal Dedicated Program. Development of Spaceports to Support Space Activities, 2017–2025 (approved by the Government of the Russian Federation on 13 Sept 2017)
- Federal Space Program of Russia for 2016–2025 (approved by the Government of the Russian Federation on 23 March 2016)
- International Space Company Kosmotras (2019a) Reliability. <http://www.kosmotras.ru/en/reliability/>. Accessed 29 March 2019
- International Space Company Kosmotras (2019b) Dnepr launch record. <http://www.kosmotras.ru/en/zapuski/>. Accessed 29 March 2019
- Khrunichev State Research, Production Space Center (2019) Rocket launch vehicle. <http://www.khrunichev.ru/main.php?id=43>. Accessed 29 March 2019
- Kommersant (2010) Sea launch to finish in Russia. <https://www.kommersant.ru/doc/1364744>. Accessed 29 March 2019
- Lenta.ru (2007) The Governor of the Amur region agreed to close the Svobodny Cosmodrome. <https://lenta.ru/news/2007/03/14/cosmodrome/>. Accessed 29 March 2019
- Lenta.ru (2015) The Ukraine bans the supply of components for the Rocket launch vehicle to Russia. <https://lenta.ru/news/2015/02/12/rokok/>. Accessed 29 March 2019
- Lenta.ru (2019) The “minimum” cost of the Russian super heavy rocket is revealed. <https://lenta.ru/news/2019/03/25/iss/>. Accessed 29 March 2019
- Main Provisions of the Principles of State Policy in the Field of Space Activities, till 2030 and Further Prospect (approved by the President of the Russian Federation on 19 April 2013)
- NPO Mashinostroyeniya (2019) Strela rocket space complex. <http://www.npomash.ru/activities/en/krk.htm>. Accessed 29 March 2019
- Opening remarks by Dmitry Medvedev, Prime Minister of Russia, at the meeting on the financial and economic condition of Roscosmos State Corporation and its subordinate organizations January 23, 2019. <http://government.ru/news/35460/>. Accessed 29 March 2019
- Progress Rocket Space Center (2014–2018) Soyuz-FG launch vehicle. [https://www.samspace.ru/products/launch\\_vehicles/m\\_soyuz\\_fg/](https://www.samspace.ru/products/launch_vehicles/m_soyuz_fg/). Accessed 29 March 2019
- Ria Novosti (2019) Dmitriy Rogozin has commented on the first stage works on construction of Vostochny cosmodrome. <https://ria.ru/20190322/1552036765.html>. Accessed 29 March 2019
- Roscosmos State Corporation (2019a) The Breeze-series upper stages. <https://www.roscosmos.ru/450/>. Accessed 29 March 2019
- Roscosmos State Corporation (2019b) RS-20. <https://www.roscosmos.ru/470/>. Accessed 29 March 2019
- Rossiyskaya Gazeta (2014) 33 satellites of the “Satan”. Nuclear missiles work for peaceful space. <https://rg.ru/2014/06/20/zapusk-site.html>. Accessed 29 March 2019
- Telesputnik (2019) Proton-M will compete with the falcon rocket by saving on pre-launch training. [https://telesputnik.ru/materials/tekhnika-i-tekhnologii/news/proton-m-budet-konkurirovat-s-m-falcon-za-schet-ekonomii-na-predstartovoy-podgotovke/?utm\\_source=newsletter&utm\\_medium=email](https://telesputnik.ru/materials/tekhnika-i-tekhnologii/news/proton-m-budet-konkurirovat-s-m-falcon-za-schet-ekonomii-na-predstartovoy-podgotovke/?utm_source=newsletter&utm_medium=email). Accessed 29 March 2019
- Vzglyad Business Newspaper (2016) The government approved the Federal Space Program for 2016–2025. <https://vz.ru/news/2016/3/17/800054.html>. Accessed 29 March 2019
- Zvezda (2018) Specialists from Khrunichev space Center have reported when the reusable version of Angara launch vehicle will go into production. <https://tvzvezda.ru/news/opk/content/201801281917-qhyv.htm>. Accessed 29 March 2019



# Institutional Space Security Programs in Europe

# 61

Ntorina Antoni, Maarten Adriaensen, and Christina Giannopapa

## Contents

Introduction .....	1192
The European Union .....	1193
The European Union Space and Security Institutions .....	1194
European Union Space Security Activities/Programs .....	1198
The European Space Agency: ESA .....	1207
ESA Space Security Status .....	1207
ESA Space Security Activities/Programs .....	1208
North Atlantic Treaty Organization: NATO .....	1215
NATO Space and Security Status .....	1215
NATO Space and Security Activities/Programs .....	1216
Conclusion .....	1220
References .....	1221

## Abstract

European institutional actors are increasingly involved in space and security programs. This chapter addresses the programs of institutional actors engaging in space and security activities in Europe, namely, the European Union (EU), the European Space Agency (ESA), and the North Atlantic Treaty Organization (NATO). The recent policy developments in these organizations and European

---

N. Antoni (✉)

Eindhoven University of Technology, Eindhoven, The Netherlands

e-mail: [ntorina.antoni@gmail.com](mailto:ntorina.antoni@gmail.com)

M. Adriaensen · C. Giannopapa

European Space Agency (ESA), Paris, France

e-mail: [maarten.cm.adriaensen@gmail.com](mailto:maarten.cm.adriaensen@gmail.com); [christina.giannopapa@esa.int](mailto:christina.giannopapa@esa.int)

© Springer Nature Switzerland AG 2020

K.-U. Schrogl (ed.), *Handbook of Space Security*,

[https://doi.org/10.1007/978-3-030-23210-8\\_112](https://doi.org/10.1007/978-3-030-23210-8_112)

1191

countries as described in ► [Chap. 23, “Strategic Overview of European Space and Security Governance”](#) of this Handbook are inextricably intertwined with the national programs of the European Member States that are presented in the corresponding chapters of Space and Security Programs in the Largest, Medium-Sized and Smaller European Countries. This chapter includes space activities and programs in the fields of Earth observation (EO); Satellite Communication (SATCOM); Positioning, Navigation and Timing (PNT); and Space Situational Awareness (SSA).

---

## Introduction

The increased need for security in Europe and for Europe’s space activities had led to several activities and programs developed by institutional actors in the space and defense sectors, towards the strengthening of European security and defense.

In this context, the European Union (EU), the European Space Agency (ESA), and their respective Member States have strengthened their existing partnerships and have established new ones with security stakeholders in Europe. In addition, the North Atlantic Treaty Organization (NATO) has recently adopted a space policy for security and defense purposes. Hence, the main institutional actors addressed in this chapter are the European Union (EU) and the European Space Agency (ESA), while it is worth addressing the activities and programs that NATO has in place.

The EU is a supranational organization composed of 28 Member States. Article 189 of the Treaty on the Functioning of the European Union is the legal basis for EU space affairs. The Council of the EU, the European Parliament, and the European Commission (EC) play an important role in the EU space program. The EU Global Strategy, adopted by the European Council in June 2016, the European Commission Space Strategy for Europe, launched in October 2016, and the European Defence Action Plan 2016 all stress the importance of having access to European Governmental Satellite Communications (GOVSATCOM) capabilities. More recently, in June 2018 the EU has presented the proposal for a regulation for a Space Programme for the EU.

ESA is an intergovernmental organization with 22 Member States (Canada and Slovenia are Associated States) with its mandate enshrined in the 1975 ESA Convention. ESA has increasingly contributed to space security in and from space as reflected in the Council Document “Elements of ESA’s Policy on Space and Security” issued in June 2017 (Giannopapa et al. 2018). The document acknowledged ESA’s involvement in space and security activities and provided for the guiding principles of ESA’s future involvement in the domain of space and security in view of strengthening the dialogue with Member States and supporting the current and future activities of the Agency. In December 2019, the Council at the Ministerial level adopted the safety and security pillar and associated programs.

NATO is an international organization with 29 Member States. The 2010 NATO Strategic Concept identifies collective defense, crisis management, and cooperative

security as the essential core tasks that NATO must continue to fulfil to assure the security of its members. In June 2019, NATO adopted a new overarching Space Policy. While both the NATO space strategy and the political designation of space as a potential warfighting domain, in November 2019 NATO recognized space as an operational domain.

Accordingly, this chapter addresses space activities and programs in the fields of Earth observation, Satellite Communication (SATCOM), Global Navigation Satellite Systems (GNSS), Space Situational Awareness (SSA), space transportation, satellite operations, and detection, tracking, and warning. Cross-domain applications, general research and technology development, and business development and technology transfer are not structurally analyzed.

---

## The European Union

The EU is a supranational organization composed of 28 Member States (27 now at the time of the writing because of Brexit). The EU legal basis for defense affairs is situated in Articles 42 and 43 of the Treaty on European Union, while the EU legal basis for space is situated in Article 189 of the Treaty on the Functioning of the European Union. Both the Council of the EU, the European Parliament, and the European Commission play an important role in the EU space program. The EU has been increasingly investing in European space programs. The EU implements the space component development phase of its two flagship programs Copernicus and the European Geostationary Navigation Overlay Service (EGNOS)/Galileo via delegation agreement with ESA. The 2021–2027 proposed by the European Commission space budget of €16 billion for the EU Space Programme Components and the EU Agency for Space (not including space research under Horizon Europe) consists of (European Commission 2018a):

- Galileo and EGNOS: €9.7 billion
- Copernicus: €5.8 billion
- Space Surveillance and Tracking (SST) and Governmental Satellite Communication (GOVSATCOM): €500 million

Additionally, on 9 April 2019, the Directorate-General for Communications Networks, Content and Technology (DG Connect) of the European Commission and the European Space Agency (ESA), signed a technical agreement to collaborate in designing a Quantum Communication Infrastructure (QCI) from Europe. The Euro QCI aims to represent the next generation of ultra-secure communications in Europe, allowing information to be transmitted and stored ultra-securely, linking critical data and communication assets all over the continent. The Euro QCI is expected to consist of components on earth and in space and is expected to boost Europe's capabilities in cybersecurity and communications. The European Space Agency would be the system architect on behalf of the Commission on the space component.



## The European Union Space and Security Institutions

### European Commission

The European Commission has released its regulatory proposal for the EU space program for the period 2021–2027 on 6 June 2018 (European Commission 2018b). This is in line with the Communication that the European Commission released in October 2016 on its Space Strategy for Europe. At the time of the writing, the proposal is under discussions with the Council of the EU. The European Commission has released its regulatory proposal for the EU Research Framework Programme in the period 2021–2027 (Horizon Europe) on 7 June 2018. Space research is included in the Cluster Digital, Industry, and Space (15 billion EUR in total – space amount to be determined). The proposal refers to Galileo/EGNOS, Copernicus, secure satellite communications, SSA, 5G and Next Generation Internet (NGI), non-dependence and sustainability of the supply chain, new innovative technologies, and space science (European Commission 2019a). On 30 September 2019, the European Commission and the European Space Agency (ESA) organized a joint industry day on “quantum communication infrastructure (QCI) for Europe – space segment” to share and discuss various options for potential space infrastructure for different use cases with QCI stakeholders. This was followed by a declaration that until early 2020 has been signed by 20 EU Member States (European Commission 2019b). This Declaration builds on the technological advances made by the EU space programs and by ESA to significantly boost Europe’s capabilities in optical communications and cybersecurity. One of their objectives is to use satellite technologies for delivering Quantum Key Distribution (QKD) services (a technology that uses the principles of quantum mechanics to perform cryptographic tasks), which are not achievable by terrestrial solutions alone (European Commission 2019b).

Space is further relevant in the areas of Open Science and Open Innovation (Space Equity Pilot in Horizon 2020, SME-instrument). The European Commission is in the process of elaborating a Strategic Research and Innovation Agenda (SRIA) for Space Technology under Horizon Europe, taking benefit from work performed in the Space Policy Expert Group (SPEG), Steering Group of the ESA-Commission-EDA Joint Task Force on Critical Space Technologies and Harmonisation activities and the Working Group of the ASD-Eurospace Space Technologies: European Partnership PLATFORM (STEPP) Project.

Within the European Commission, the Directorate-General (DG) for Internal Market, Industry, Entrepreneurship and SMEs (DG GROW) held the main responsibility for space activities of the EU. In addition to GROW, also the DG for Communications Networks, Content and Technology (DG CONNECT), the Joint Research Centre (JRC) in the Directorate E – Space, Security and Migration, the DG For European Civil Protection and Humanitarian Aid Operations (DG ECHO), the DG for Migration and Home Affairs (DG HOME), the DG for Maritime Affairs and Fisheries (DG MARE), the DG for Mobility and Transport (DG MOVE), the European Political Strategy Centre (EPSC), and the DG for Research and Innovation (RTD), are concerned.

At the end of 2019, a new DG for Defence, Industry and Space (DEFIS) has been realized with responsibilities that were previously covered by DG GROW. DEFIS is created under the responsibility of the Commissioner for Internal Market. The Commissioner is also responsible for DG CONNECT and DG GROW (European Commission 2019a). The new DG will most likely (OSW 2019):

- Implement the European Defence Fund
- Ensure an open and competitive European defense equipment market and enforcing EU procurement rules on defense
- Implement the Action Plan on Military Mobility (in collaboration with the DG Mobility and Transport)
- Foster an innovative space industry in the EU
- Implement the EU Space Programme

Horizon2020 is the EU Framework Programme for R&D and innovation for the period 2014–2020. It builds further on FP7 and brings together the innovation parts of the Competitiveness and Innovation Framework Programme (CIP) and the EU Institute of Innovation and Technology (EIT). The objective is to maximize the contribution of the EU funded research and innovation to sustainable growth and jobs.

In 2017, the Commission established a SPEG subgroup in view of an improved coordination and policy-based approach regarding space technologies and associated actions to be supported by the Union. The SPEG subgroup is composed of representatives from the EU Member States and nominated observers from the European Space Agency and the European Defence Agency (ESA 2017a).

### **Political and Security Committee**

The Political and Security Committee (PSC) meets at the ambassadorial level as a preparatory body for the Council of the EU. Its main functions are keeping track of the international situation and helping to define policies within the Common Foreign and Security Policy (CFSP) including the Common Security and Defence Policy (CSDP). It prepares a coherent EU response to a crisis and exercises its political control and strategic direction. The European Union Military Committee (EUMC) is the highest military body set up within the Council. It is composed of the Chiefs of Defence of the Member States, who are regularly represented by their permanent military representatives. The EUMC provides the PSC with advice and recommendations on all military matters within the EU. In line with relevant Council Conclusions, the European Commission restated its determination to closely collaborate with the European External Action Service (EEAS), the European Defence Agency (EDA), and the EU SatCen, together with Member States and the European Space Agency (ESA) “to explore possible dual-use synergies in the space programs.”

### **European External Action Service**

Established in 2011, the European External Action Service (EEAS) is the EU diplomatic service and manages the EU’s diplomatic relations with other countries

outside the bloc and conducts EU foreign and security policy. Within the Security Policy Office (SECPOL) under the Deputy Secretary General for CSDP and Crisis Response, the Security Policy and Space Policy Unit (SECPOL 3) is charged with space affairs in the EEAS, working side by side with the EEAS Space Task Force led by the Special Envoy for Space. Complementing SECPOL, space is relevant in the frame of the INTCEN (EU Intelligence and Situation Centre), the CMPD (Crisis Management and Planning), and the CPCC (Civilian Planning and Conduct Capabilities). The EU Military Staff (EUMS) is also involved in space with stakeholders in the EUMS MPCC (Military Planning and Conduct Capability). As the EU diplomatic service, the EEAS focuses on space security, safety, and sustainability in a global multilateral context (the post Code of Conduct) and in the emerging domain of economic diplomacy including space. The EU Intelligence Analysis Centre (INTCEN) (formerly known as SITCEN, and its origins go back to the WEU) is a Directorate at the EEAS. Its mission is to provide intelligence analyses, early warning and situational awareness to the High Representative and to the European External Action Service, to the various EU decision-making bodies in the fields of the CFSP and CSDP, and counterterrorism, as well as to the EU Member States.

### **European Defence Agency**

EDA is an EU Agency that promotes and facilitates integration between member states within the EU's Common Security and Defence Policy (CSDP). The EDA is headed by the High Representative (HR), and reports to the Council of the EU. EDA is Europe's defense capability development actor. EDA and EEAS together form the Secretariat for Permanent Structured Cooperation (PESCO). EDA performs the Coordinated Annual Review on Defence (CARD). The EDA Capability Development Plan (CDP) was approved by EDA Steering Board in June 2018 (EDA 2018a). EDA is contributing to the preparation of the European defense research program (EDRP) and is involved in the preparation of the European defense industrial development program (EDIDP). The PESCO participating Member States have committed to use EDA as the European forum for joint capability development and consider OCCAR as preferred collaborative program management organization. An initial list of 17 projects to be developed under PESCO was adopted by the Council on 6 March 2018. A second batch of 17 projects to be developed under PESCO was adopted by the Council on 19 November 2018. And finally, a third batch of 13 additional projects to be developed under PESCO was adopted by the Council on 12 November 2019 (EDA PESCO 2018). EDA activity in the domain space is indispensable as space-based communication, situational awareness, and navigation and earth-observation capabilities play an increasingly critical role in security and defense. Satellite reconnaissance is one of the key functions allowing countries to gather information about military build-up or movement of troops worldwide. Precision-guided munitions, missile warning and launch detection systems, and space-based missile defense systems are other examples of space enabled defense capabilities (EDA 2017a).

The importance of space assets and applications for defense capabilities is reflected in the revised CDP approved by the EDA Steering Board in June 2018 (EDA 2018c). Space-related priorities are included notably in the so-called priority areas of Space Based Information Services (Earth Observation (EO); Positioning, Navigation and Timing (PNT); Space Situational Awareness (SSA); Satellite Communication); Information superiority (Radio Spectrum Management; Tactical Communication and Information System (CIS); Information management; Intelligence, Surveillance and Reconnaissance (ISR) capabilities); Air Superiority (i.a. Ballistic Missile Defence) and; cyber defense in space. (EDA 2018a). With regard to synergies between civil and defense research and technology (R&T), the R&T mandate of EDA includes the promotion of collaboration with other stakeholders. EDA, ESA, and the European Commission have cooperated in the frame of “Critical Space Technologies for European Strategic Non-Dependence” (ESA 2018c). ESA and the EDA are also cooperating in the development of new AI-based capabilities in the field of guidance, navigation, and control (GNC) – knowing where an asset is and steering where it is going. Advanced, autonomous GNC is set to become an indispensable element of ambitious future space missions such as rendezvousing with asteroids and comets or the active removal of hazardous space debris from orbit (EDA 2020b). EDA is the defense community facilitator towards the European Commission and EU Agencies and acts as the interface upon Member States’ request, exploiting wider EU policies to the benefit of defense and acting as a central operator regarding EU funded defense-related activities. In that regard, EDA has an indispensable role, in support of its Member States, in harmonizing military user requirements for all European space programs.

### **European Union Satellite Centre**

The European Union Satellite Centre (Satcen), previously EUSC and initially founded as the Western European Union Satellite Centre, is an EU Agency that supports the EU’s decision-making in the field of the Common Foreign and Security Policy (CFSP), including crisis management missions and operations, by providing products and services resulting from the exploitation of relevant space assets and collateral data, including satellite and aerial imagery, and related services. SatCen’s director reports to a governing board chaired by the EU’s High Representative for Foreign Affairs and Security Policy (HR/VP). The EU Satcen provides high-level geospatial analyses based on satellite imagery to the EEAS, the EU Member States and to some international organizations such as NATO, the International Atomic Energy Agency (IAEA), the Organization for Security and Co-operation in Europe (OSCE), and the Organisation for the Prohibition of Chemical Weapons (OPCW). Based on the 2014 Council Decision, SATCEN shall support the decision-making and actions of the Union in the field of the CFSP and the CSDP, including European Union crisis management missions and operations, by providing, at the request of the Council or the HR, products and services resulting from the exploitation of relevant space assets and collateral data, including satellite and aerial imagery, and related services (Council of the EU 2014). Its main users are the European External Action Service (EEAS), Member States and international organizations.

Satcen's mission is aimed at providing the exploitation of relevant space assets and collateral data and services. Satcen uses open source data, commercial satellite imagery, and governmental imagery sensors; Helios II, Cosmo-SkyMed, SAR-Lupe. In 2016, the classified COSMO-SkyMed link between SatCen and the Italian authorities was installed and declared operational. SatCen has since the ability to order and download classified COSMO-SkyMed products in an easy, secure, and fast manner. The SAR-Lupe classified link between SatCen and the German ground segment is fully operational and is used to place requests and download SAR-Lupe classified imagery (Satcen 2016). Satcen performs delegated operation on behalf of the European Commission: Copernicus in Support to EU External Action (SEA), Copernicus Border Surveillance (in support to FRONTEX), Copernicus Service Evolution (SEA and border surveillance), and Initial Space Surveillance and Tracking (SST) services. Satcen bridges the gap between research and applications in the field of space and security, operating as a dual-use agency serving civil and military users. Satcen priorities for space research include requirements for next-generation Intelligence-Surveillance-Reconnaissance (ISR), geoportals for CSDP missions and EEAS users, cross-cutting dual-use applications using EU space program assets, the use of artificial intelligence for remote sensing applications and deployment of cloud-based solutions for secure data access and distribution, and use of satcom solutions for dissemination of geospatial data and products.

## **European Union Space Security Activities/Programs**

### **Earth Observation- EO**

#### **Copernicus Operational Services**

Copernicus is the European Flagship Programme for monitoring the Earth. It is coordinated and managed by the European Commission. The services address six thematic areas: land, marine, atmosphere, climate change, emergency management, and security. They support a wide range of applications, including environment protection, management of urban areas, regional and local planning, agriculture, forestry, fisheries, health, transport, climate change, sustainable development, civil protection, and tourism. The Copernicus legal structure between the EU and ESA is composed of the following elements: the Copernicus EU Regulation, the European Commission Delegation Decision, the EU-ESA Agreement, and ESA contracts within the ESA name. As part of the Copernicus Programme, the European Commission and ESA have awarded in July 2018 an Airbus-led consortium a contract for the provision of satellite-based seamless coverage of the whole of Europe at very high-resolution. The consortium includes Airbus Defence & Space, Planet, Deimos Imaging, IGN-France, and space4environment.

The missions in the Copernicus Space Component are: Sentinel-1; Sentinel-2; Sentinel-3; Precursor Sentinel-4; Sentinel-5; and Sentinel-6. The European Commission DG GROW delegates Copernicus activities to the European Environment Agency (EEA), the European Maritime Safety Agency (EMSA), the European

Border and Coast Guard Agency (Frontex), Satcen, ESA, the European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT), the European Centre for Medium-Range Weather Forecasts (ECMWF), and Mercator Ocean (European Commission DG GROW Website). Frontex and EMSA are European Commission decentralized agencies. The operational services of Copernicus are situated in three major axes: Border surveillance (Frontex); Maritime surveillance (EMSA); Support to External Action (Satcen).

Frontex supports, coordinates and develops European border management in line with the Treaties including the Charter of Fundamental Rights of the EU as well as other international obligations. Frontex coordinates operational and EU measures to jointly respond to exceptional situations at the external borders. Frontex develops capacities at Member States and European level as combined instruments to tackle challenges focusing of migration flows, but also contributing to fight cross-border crime and terrorism at the external borders. Frontex builds the capacities and capabilities in the Member States aiming at develops a functioning European Border and Coast Guard. In November 2015 Frontex signed a Delegation Agreement with DG GROW amounting to €47.5 million for the period 2015–2020 to implement the Border Surveillance component of the Copernicus Security Services. The objective of this component is to provide increased situational awareness when responding to security challenges at the external border through detection and monitoring of cross-border security threats, risk assessment and early warning systems, and mapping and monitoring (Council of the EU 2019a).

EMSA supports, coordinates and develops European maritime safety and security, including prevention of and response to pollution. EMSA Services are offered to all EU and EFTA Member States in accordance with existing access rights and provide enhanced features for, among others, environmental monitoring, search and rescue, and traffic monitoring purposes. It allows Member States to make full use of the integrated vessel reporting information from terrestrial and satellite Automatic Identification System (AIS), Long-Range Identification and Tracking (LRIT), Vessel Monitoring System (VMS), as well as national vessel position data such as coastal radar, patrol assets, and leisure craft. EMSA provides maritime border control support to Frontex under the auspices of the European Border Surveillance System (Eurosur). Vessel information originates from both terrestrial and satellite-based systems as well as other available positioning data and are correlated against satellite aperture radar and optical imagery derived vessel detections. EMSA further provides operational support for the European Fisheries Control Agency (EFCA) coordinated Joint Deployment Plan operations (JDP) for fisheries activities in the Mediterranean, North & Eastern Atlantic and the North Sea waters. It includes a real time maritime awareness operational picture fusing and correlating VMS, terrestrial AIS, satellite AIS, and LRIT position reports together with visual sightings, as well as establishing a common fishery vessel registry (EMSA 2014).

### **EDA Activities and Programs**

In July 2016, the EDA and Satcen formalized their close and fruitful cooperation, already in place since 2004, with an exchange of letters. With the exchange of letters,

the EDA and SATCEN establish a more structured cooperation meaning that they will even more focus on activities of mutual interest, such as studies, workshops, projects, and programs. EDA and SATCEN have also identified specific cooperation areas such as imagery exploitation, geospatial analysis and applications, future space-based earth observation systems, cyber defense, Big Data exploitation in the space and security domain, space situational awareness, or maritime surveillance. The two Agencies will also develop a joint roadmap for cooperation detailing the activities of common interest as included in the respective work programs. The roadmap will be updated annually (EDA 2017a).

In addition, the SULTAN (Persistent Surveillance Long Term Analysis) study was a 2014–2015 cooperative study from EDA and ESA executed by Airbus Defence & Space, aimed at identifying potential options to enhance collection capabilities in Imagery Intelligence (IMINT) through innovative and technologically feasible solutions, able to deliver an operational capability at 2025–2030 timeframe, to meet the need of persistent surveillance of wide areas in defense and security operations. To this extent, the project has provided analysis and description of operational scenarios, technology roadmaps, rough estimation of cost, time schedule and respective merits of assets/systems based on geostationary satellite systems, constellations of optical and radar small/mini satellites in low earth orbit, High Altitude Pseudo-Satellite Systems (HAPS), and Remotely Piloted Aircraft Systems (RPAS). The study represented a significant step in the EDA Intelligence, Surveillance and Reconnaissance capability development process (analysis, identification and selection of IMINT capacities). The dual-use dimension of the surveillance systems and the joint requirement analysis performed on security and defense scenarios could also be used in the framework of future activities in cooperation with the European Commission (EDA 2016a).

Moreover, EDA has a Project Team Space-Based Earth Observation (PT SBE0). The PT regroups all the EDA activities concerning Space Based Earth Observation and is currently elaborating a Common Staff Requirement (CSR) for Earth Observation Requirements in the time frame 2025–2030, following a Common Staff Target (CST) approved in July 2017. This task is executed in cooperation with Member States representatives, European Military Staff and the European Satellite Centre, as well as taking benefit of the experience and expertise at ESA and the European Commission. EDA is investigating the use of Copernicus for defense users, in collaboration with the European Commission DG GROW (ESA 2017a).

The EDA-Satcen cooperative project Radar Imagery Applications Supporting Actionable Intelligence (REACT) has enhanced imagery operators' abilities to manage the complexity of working with radar imagery, especially by providing practical information on the various steps of the workflows to be followed and established credible working procedures for radar imagery exploitation. The work undertaken also allowed us to evaluate new tools and sophisticated algorithms for radar imagery exploitation, such as Automatic Target Detection & Recognition. After the initial REACT Study, EDA has a follow-up activity REACT 2 study on imagery exploitation activities. Working again with the EU SatCen, the focus will be on making SAR IMINT workflows more efficient through defining operating

procedures and the use of business process workflow tools. One key objective is to increase the speed of analysis within the radar IMINT tasking cycle (EDA 2017b).

EDA and ESA have signed an Implementing Arrangement on cooperation on Earth observation requirements in the time frame 2025–2030. EDA and ESA will implement a joint study to be contracted in 2018, elaborating mission concepts and a roadmap of technologies needed for future security Earth observation missions. This study will feed into the EDA CSR process (EDA 2018b).

## **Satellite Communications: SATCOM and Cross-Domain Applications**

### **Governmental Satellite Communications: GOVSATCOM**

The European Commission has proposed the establishment of a new EU Space program component aimed at pooling and sharing of secure governmental satellite communications (European Commission 2018b). The EU Global Strategy, adopted by the European Council in June 2016, the European Commission Space Strategy for Europe, launched in October 2016, and the European Defence Action Plan which followed the subsequent month all stress the importance of having enough access to European GOVSATCOM capabilities. Furthermore, in March 2017, the Council’s Political and Security Committee has endorsed the document of High Level Civil-Military User Needs for GOVSATCOM, thus further consolidating civil-military synergies in the field (EDA 2017c).

The November 2013 Steering Board at Ministerial level endorsed EDA’s proposal and roadmap on developing a future GOVSATCOM capability in support of national defense efforts. On this basis, the 19 December 2013 European Council, “committed to delivering key capabilities and addressing critical shortfalls through concrete projects by Member States, supported by the European Defence Agency,” welcomed “preparations for the next generation of Governmental Satellite Communication through close cooperation between the Member States, the Commission and the European Space Agency.” Following this mandate delivered by EU Heads of States and Governments, EDA has developed in 2014 the defense needs related to the use of governmental satellite communications assets (ESA 2017a).

In the frame of the 2014 EDA CDP, provision of satellite communication capabilities was agreed as a prioritized action. A landscape of SATCOM capabilities in Europe demonstrated that almost all current national assets will have to be renewed or completed before 2020/2025. In the European Council of December 2013, EDA has been mandated to support participating MS in the capability development process of the next generation of governmental satellite communications (European Council 2013). This step triggered the launch of the project preparation phase which has led to the adoption of a Common Staff Target, describing military user needs, on 4 November 2015, and through Common Staff Requirements and Business Case in March 2017. EDA Steering Board approved in February 2018 a mandate for EDA to act as facilitator in support of the Ministries of Defence within the EU GOVSATCOM Programme (ESA 2017a).



## **EU SatCom Market**

The EU Satcom Market comprises 31 contributing members. The EU SatCom Market has, since the project started in 2012, provided an efficient option to source commercially available SatCom services and from 2017, Communication and Information System (CIS) services are also added to the whole portfolio of services offered to its members. The project goals are to provide a cost effective commercial SatCom and CIS solutions for members and to reduce costs, ease access, and improve operational efficiency for members. In January 2016, the second Framework Contract was awarded to Airbus Defence & Space. In July 2017, the first Framework Contracts for Communication and Information System services were awarded to Airbus Defence & Space and Thales Communications & Security. In January 2020, the third Framework Contract for SatCom services was awarded to an Airbus Defence & Space and Marlink consortium. From the first request in 2013 up to January 2020, €35.4 million in total ordering value for SATCOM services has been placed through the framework contracts (EDA [2020a](#)).

## **EDA GOVSATCOM**

The EDA Project Team on Satellite Communications is part of the Ad Hoc working Group preparing the establishment of the EDA GOVSATCOM Demonstration Project (Pooling and sharing) to start activities in 2018. The Working Group elaborates a Project Arrangement (PA) for the GSC demo supported by a Concept of Operations (CONOPS) document that will serve as the framework for the PA. The program objectives are to demonstrate the benefits of a European dual-use approach for the development of such capability and to provide EDA Member States and European CSDP actors with access to a GOVSATCOM capability based on existing, pooled, governmental SATCOM resources. EDA is in the process of finalizing and signing with its participating Member States the Project Arrangement on the EDA GOVSATCOM demonstration project with operations to commence before the end of 2018 (EDA [2017c](#); ESA [2017a](#)).

## **EDA-ESA**

EDA and ESA signed in March 2017 an Implementing Arrangement on exploiting space-based assets to advance capabilities in Chemical, Biological, Radiological, Nuclear, and explosive (CBRNe) threats. ESA launched a feasibility study in 2017 in order to assess the technical and economic viability of deploying services based on Satellite Communications, Satellite Navigation, Earth Observation data, and/or other space assets to support CBRNe operations (e.g., catering for detection and situational awareness, prediction, early warning, and response planning) for the benefit of both institutional and commercial users. The study will eventually propose a roadmap for service(s) implementation and demonstration. The feasibility study also included an Option for ESA-EDA cooperation in order to demonstrate the benefits that the National Stakeholder Communities (NSC) in charge of combating CBRNe threats in EU Member States can get from the utilization of services integrating space and terrestrial technologies. The NSC includes different bodies

engaged with the planning and execution of actions in response to CBRNe threats (ESA 2017c).

The Administrative Arrangement between EDA and ESA signed in June 2011 provides the legal framework for cooperation projects between EDA and ESA.

## **Positioning, Navigation, and Timing: PNT**

### **Galileo**

Galileo is a fully European program. The European Commission has overall responsibility for the program, managing, and overseeing the implementation of all activities on behalf of the EU. Galileo's deployment, its design, and the development of the new generation of systems and the technical development of infrastructure is entrusted to the European Space Agency (ESA). ESA oversees the R&D phase and IOV phase and co-finances the Galileo program of about 50%. The EU remains the sole owner of the infrastructures and the services (Schrogl et al. 2015).

The four services of Galileo are: Open Service (OS), Commercial Service (CS), Public Regulated Service (PRS), and Search and Rescue Service (SAR). The Commission has delegated the operational management of the program to the GSA, which oversees how Galileo infrastructure is used and ensures that Galileo services are delivered as planned and without interruption (European Commission Galileo Website). The European Commission has set up a specific directorate for the EU Satellite Navigation Programme, under the authority of the DG GROW and two expert groups: Security Board for European GNSS (6 Working Groups) and the Search and Rescue Galileo Operations Advisory Board. The European GNSS Programme Committee (4 Working Groups) monitors and supports the European Commission activities and forms the space for dialogue for Member States. The Galileo Security Board (with 10 Working groups) with Member States representatives primarily from or on behalf of the Ministries of Transport is an advisory body supporting DG GROW in the execution of the Galileo Programme (Sitruk and Plattard 2017).

ESA is charged with the deployment of the European satellite navigation program Galileo through the so-called Galileo Deployment Delegation Agreement. The first 22 satellites of the Galileo "Full Operational Capability" phase are built by OHB (Germany) and Surrey Satellite Technology Ltd. (UK), which is producing the payloads. ESA is now being tasked with the preparation and procurement of the Transition Satellites and supporting equipment qualification activities (ESA 2018e).

Galileo has two control centers: Fucino in Italy generates the accurate navigation messages that are then broadcast through the navigation payloads, and Oberpfaffenhofen in Germany controls the constellation of satellites. A new telemetry, tracking, and command station last year was constructed in Papeete on Tahiti, in the South Pacific in 2017. Establishing Galileo's ground segment was among the most complex developments ever undertaken by ESA, having to fulfil strict levels of performance, security, and safety. Formal responsibility for the operations of this Galileo ground segment was last passed to the GSA in 2017 but ESA continues to

oversee its maintenance and growth. Galileo telemetry, tracking, and command stations are situated in the Kiruna, Redu, Kourou, Reunion, Noumea (in New Caledonia), and the Papeete sites. The ground segment also comprises a set of four Medium-Earth Orbit Local User Terminals serving Galileo's search and rescue service, at the corners of Europe and facilities for testing Galileo service quality and security – the Timing and Geodetic Validation Facility and two Galileo Security Monitoring Centres. The Launch and Early Operations Control Centers have the task of bringing new satellites to life, to be handed over to the main Satellite Control Centre in Oberpfaffenhofen within typically a week after launch. The Redu Centre in Belgium set up as Galileo's In-Orbit Test Centre, then puts these satellites through a complex set of testing and checkouts ahead of them joining the working constellation (GPS World 2018).

### **EGNOS**

EGNOS is a Satellite Based Augmentation system (SBAS), created to complement GNSS. The development of EGNOS was managed by the European Space Agency (ESA) under a tripartite agreement with the European Commission and the European Organisation for the Safety of Air Navigation (Eurocontrol). The ownership of the EGNOS assets was transferred from the ESA to the Commission in April 2009 and EGNOS officially entered service on 1 October 2009. Through a contract with the European GNSS Agency (GSA), the service is delivered by the European Satellite Services Provider, ESSP SaS, which was founded by seven air navigation service providers. The GSA has been the EGNOS Programme Manager under delegation from the Commission since 2014 and the ESA is the design and procurement agent working on behalf of the Commission. Efforts are made to extend the geographical coverage for EGNOS services in the European High North, North Africa, and the Middle East (GSA 2017).

Airbus has been selected as the main contractor to develop EGNOS V3. The contract was awarded by ESA, which manages EGNOS development under a working arrangement signed with the European GNSS Agency (GSA), in January 2018. Two EGNOS upgrade versions. EGNOS V3.1 will ensure continuity of EGNOS augmentation of GPS L1, but with a more resilient performance, while EGNOS V3.2 will support a new SBAS service, transmitting on the L5 frequency, which will augment Galileo L1/E1 – L5/E5 along with GPS (Sitruk and Plattard 2017).

### **GSA**

Unlike Copernicus, where the EU still strongly relies on ESA, EUMETSAT and national capabilities for operations, the EU has fully taken over program management for, and exploitation of EGNOS and Galileo through its executive arm, the European Commission. To deal efficiently with those new kinds of missions, it has also created a dedicated entity, the European GNSS Agency (GSA). According to the EU Proposal for a Regulation for a Space Programme for the EU, GSA will be rebranded as the new European Union Agency for the Space Program (EUSPA). EUSPA is ready to succeed and expand the current European GNSS Agency (GSA), which has been managing the EU's Galileo satellite system for 15 years (European

Commission 2018b). In addition to the development of Galileo operations, the EUSPA will manage the use of the Copernicus Earth observation satellite system, prepare the Governmental Satellite Communications (GOVSATCOM) program, and concentrate EU capacities to monitor the Earth's near surroundings (European Commission 2018b; GSA 2020).

With regard to the GSA, in its current form, it is a decentralized (or regulatory) agency of the EU and a key element of European GNSS governance. The GSA was initially set up by the Parliament and the Council through Regulation (EU) N° 912/2010, amended by the Regulation (EU) N° 512/2014 (GSA Regulation). The role of the GSA, its prerogatives, and its internal organization has changed several times since the beginning of the Galileo program. The Agency was created in 2004 to protect the public interest within the former Galileo precise point positioning (PPP) model and given with an important core of related prerogatives (concession contract implementation, security management, PRS-related activities, Member States coordination, etc.). After a drastic reduction of its role, the last regulation gave an important role back to the GSA as the entity that should progressively take charge of system exploitation. The current prerogatives of the GSA are now mainly defined by the GNSS Regulation, completed by the GSA Regulation. They are of two kinds: some prerogatives are fully owned by the GSA ("core prerogatives"), whereas others are delegated by the Commission through a delegation agreement (Sitruk and Plattard 2017).

## **Space Situational Awareness-SSA/Space Surveillance and Tracking – SST**

### **EU SST Program**

The European Commission has proposed the establishment of a new EU Space Programme component for Space Situational Awareness (SSA), meaning a holistic approach to enhance SST capabilities to monitor, track, and identify space objects; to monitor space weather; and to map and network Member States NEO capacities. The SSA Programme will build on and extend the current EU Space Surveillance and Tracking (SST) Support Framework to space weather and near-Earth objects (European Commission 2018b).

After the adoption of the decision establishing a framework on Space Surveillance and Tracking (SST) support in March 2014, the European Commission adopted, in September 2014, a first implementing act on the procedure for participation of Member States in the SST Support Framework. By mid-2015, a Consortium agreement on SST was signed between France (CNES), Germany (DLR), Spain (CDTI), Italy (ASI), and the United Kingdom (UKSA) represented by their respective space agencies (SST Consortium). They became the first Member States participating in the SST Support Framework (European Parliament 2014).

Implementing arrangements have also been concluded between the members of the SST Consortium and the EU Satcen for the delivery of SST services. Since January 2016, the Galileo, Copernicus, and Horizon 2020 programs have been supporting the SST activities aimed at the establishment and operation of the network of sensors, the establishment of the capacity to process and analyze SST data, and the establishment and operation of SST services. The upgrade and renewal

of SST sensors is also supported as part of the Horizon 2020 Space Research Programme (European Parliament 2018). The SST Decision identifies as SST Services: Collision Avoidance, In-Orbit Fragmentation and Uncontrolled Re-entry of space objects. To facilitate service provision, the Consortium and EU Satellite Centre (EU SatCen) form the so-called EUSST Cooperation. The work of the Cooperation is governed by the Implementing Arrangement signed in September 2015. Since July 2016, SatCen is providing initial SST services – generated by the SST Consortium – via the first instance of the EU SST Service Provision Portal (EUSST Website).

With a second Implementing Decision in 2016, the Commission launched the second round of Member States applications to join the SST Consortium. Three Member States (Poland, Romania, and Portugal) submitted formal applications to join the SST Consortium by the 19 August 2017 deadline and the procedure should be completed in 2018. The participation of new Member States can help to increase the performance of EU SST. Eight other Member States (Austria, Croatia, Finland, the Czech Republic, Greece, Latvia, Slovakia, and Sweden) expressed their intention to collaborate with the SST Consortium as participating entities in the implementation of the future grants. Private sector contributes to the EU SST, mainly as technology and data provider, and does not participate in the EU SST governance (Council of the EU 2018).

The SST Decision recognizes the sensitive nature of SST and leaves the implementation and management of the EU SST capability to the participating Member States, with assets owned at national level. The Commission's involvement in 2014–2017 was mostly related to monitoring the procedure for Member States' participation, executing grants, interacting informally with the SST Consortium, and drawing up the 2017–2020 coordination plan. The SST Consortium governance structure involves work in steering, technical, and security committees and project and financial coordination, with decisions being taken by unanimity. Most decisions, including those concerning the program management, are taken in the steering committee, where the Commission is an observer since 2017. The coordination committee – SST Consortium and SATCEN – is responsible for the governance of the SST Cooperation (Council of the EU 2018).

EU grants have financed EU SST activities in three main areas: EU SST service provision (1SST); the networking of assets and coordination of actions (2SST); and the upgrade of existing, and development of new, SST assets (3SST). A total of €167.5 million has been allocated for 2015–2020 through various grants under the Copernicus, Galileo, and Horizon 2020 programs, out of which around €70.5 million to implement the actions of the SST Decision (1SST and 2SST grants) and €97 million for the sensors' upgrades (3SST). The activities described in this report were co-financed by the 2015 grants, which were subject to administrative closure in December 2017. The 2016–2017 grants signed in December 2017 should ensure the continuity of the activities and the transition to more comprehensive and effective EU SST services. The topics of Horizon 2020 calls for grants in 2018–2020 were published in 2017. Delivery of

three initial SST services started on 1 July 2016: – conjunction analysis and warning (CA), re-entry analysis and information (RE), fragmentation analysis (FG) (Council of the EU 2018).

### **Other Activities**

EDA has concluded in 2016 a study on the Recognised Space Picture (RSP) in cooperation with Satcen. This study aimed at developing a common understanding for an RSP Display focusing on visualization aspects, proposing a draft Operational Concept and analyzing external interfaces and interoperability aspects for the benefit of EU Member States.

The Political and Security Committee of the EU (PSC) adopted in October 2011 a unified set of European Space Situational Awareness (SSA) high-level civil-military user requirements. ESA in the framework of its SSA preparatory program had defined the civil SSA mission requirements (ESA SSA Mission Requirements (MRD) – SSA-GEN-RS-MRD-1000, issue 3.0, dated 29/04/2011), which were concurred by its Member States and approved by its Executive while the EDA had defined military SSA requirements (EDA Common Staff Target (CST) 25 March 2010 – EDA SBD 2010–07), which were approved by the European ministries of defense who compose its Steering Board (Council of the EU 2019b).

After proactive USA positioning in the frame of the International Civil Aviation Organization (ICAO), the European Commission is investigating the so-called new entrants including balloons, solar planes, supersonic planes, suborbital vehicles, and High Altitude Pseudo Satellites (HAPS) HAPS. These are all situated in altitudes above flight level (FL600) and below space (100 km or the Karman Line). Higher Airspace Traffic management (HATM) is considered on top of the existing Air Traffic Management. There have been several interactions among the European Commission, Eurocontrol, the European Aviation Safety Agency (EASA), ESA, EDA, and GSA (Eurocontrol 2019).

---

## **The European Space Agency: ESA**

### **ESA Space Security Status**

ESA is an international organization with 22 Member States with its mandate enshrined in the ESA Convention. ESA is headed by its Director-General who reports to the ESA Council. ESA's mission is to shape the development of Europe's space capability and ensure that investment in space continues to deliver benefits to the citizens of Europe and the world. ESA programs are funded through mandatory and optional programs, funded by GDP-scale-based contributions to the Level of Resources and voluntary Member States' subscription to programs, respectively. The 2019 ESA budget amounts to €6.68 billion (ESA 2019a).

ESA is increasingly contributing to space security in and from space. The Council Document "Elements of ESA's Policy on Space and Security" acknowledged ESA's involvement in space and security activities and provided for the guiding principles

of ESA's future involvement in the domain of space and security in view of strengthening the dialogue with Member States and supporting the current and future activities of the Agency (ESA 2017b). It is the ambition of the ESA to exploit the potential of space in supporting safety and security matters. This ambition is reflected in the four programmatic pillars of the Agency:

- Science and Exploration (scientific program and human and robotic exploration and science support)
- Applications (Earth observation, telecommunications, navigation, and integrated applications)
- Enabling and Support (space transportation, technology development, operations)
- Safety and Security (safety and security in and from space) (ESA 2018a)

Resulting from a mandate given to ESA DG at the Ministerial Council 2016, and the decisions of Member States at the Ministerial Council 2019, ESA has recently adopted a safety and security programmatic pillar with associated program proposals (ESA 2019b).

The EU and ESA signed a Joint Statement on Shared Vision and Goals for the Future of European Space on 26 October 2016. EU and ESA emphasized their intention to reinforce their cooperation in the future as foreseen in the ESA/EU Framework Agreement of 2004 (ESA 2016).

ESA has an Administrative Arrangement in place with EDA since June 2011. Formal cooperation agreements (including exchange of letters) has been implemented for Unmanned Aircraft System (UAS); Remotely Piloted Aircraft Systems (RPAS); Chemical, Biological, Radiological, Nuclear, and high yield Explosives (CBRNe); Cyber Defence for Space; Cyber Defence Training and Exercise; GOVSATCOM; Unmanned Maritime Systems (UMS); Earth Observation Requirements (EDA 2016b).

Furthermore, the cyber defense for space cooperation provides that EDA and ESA will perform a joint study, in two phases: A first phase to identify and priorities critical space technologies which present vulnerabilities with respect to cyber threats, and a second phase to jointly develop and implement initial solutions to address such vulnerabilities. This cooperative effort seeking to maximize dual-use synergies builds upon work already carried out respectively by both ESA and EDA. ESA has also an Administrative Arrangement in place with Satcen since January 2018.

## **ESA Space Security Activities/Programs**

### **Earth Observation: EO**

ESA's Earth Observation program consists of: Earth Observation Envelope Programme (EOEP), the Earth Watch, the GMES Space Component, the Meteosat Third Generation (MTG), and the MetOp Second Generation (MetOp-SG).

At the ESA Ministerial Council 2019, it was agreed that substantial reorientation of ESA's Earth observation (EO) programs into three groups (Future EO, Operational EO, and Customised EO) to reinforce Europe's global leadership in this fast-evolving domain through the implementation of an innovative and competitive set of activities in order to serve European science and business, and fulfil societal objectives. Accordingly, the Future EO program, formerly the Earth Observation Envelope Programme (EOEP), is the backbone program that develops Earth Explorer missions as well as science and technology for all Earth observation missions conducted by ESA and its partners. The Ministers agreed to support the creation of new Scout and  $\Phi$ -sat missions to develop opportunities in the NewSpace domain. In addition, it was considered important to make full use of new technologies and methods such as artificial intelligence, big data analytics, and High-Altitude Platform Stations (HAPS) (ESA 2019b).

Operational EO comprises meteorological missions and Copernicus, the latter conducted through the successful partnership between the European Union and ESA that will focus, in the framework of ESA's Copernicus Space Component (CSC) Programme, on the development of six new Sentinel missions and the related ground segment, with a view to providing critical data and information to support European policy priorities and EU user requirements related, for example, to climate change, agriculture, biodiversity, the Arctic, Atlantic and Africa (ESA 2019b).

### Copernicus

Regarding EU space programs, the fundamental Agreement between the EU represented by the EC and ESA on the implementation of the Copernicus Programme including the ownership of Sentinels of 28 was signed in October 2014 (ESA 2018b). An amendment to the 2014 Copernicus Agreement was by the EU and ESA in January 2019, adding €96 million to ESA's space component budget for Copernicus. This additional contribution covers ESA's additional tasks such as the development of the Copernicus Sentinel-6 mission and the new European Copernicus Data Access and Information Services. In total, the budget for the Copernicus space component amounts to €3.24 billion for the 2014–2021 period. While the European Union leads the Copernicus program, ESA develops and builds the dedicated Copernicus Sentinel satellites. It also operates some of the missions and ensures the availability of data from other partners (ESA 2019d).

The Copernicus Space Component comprises two types of satellite missions, ESA's families of dedicated Sentinels and missions from other space agencies, called Contributing Missions. A unified ground segment, through which the data are streamed and made freely available for Copernicus services, completes the Space Component. ESA is establishing a mechanism to integrate, harmonize, and coordinate access to all the relevant data from the multitude of different satellite missions. This is being carried out in close cooperation with national space agencies Eumetsat and where relevant with owners of non-European missions contributing to the Copernicus objectives (ESA Copernicus Website). While the deployment of the first generation of Sentinels was completed, the ESA Member States at Ministerial Council 2019 agreed to contribute €1.8 billion for the expansion of the Copernicus



Space Component (CSC Expansion program). The six new potential Copernicus Sentinel missions, so-called High Priority Candidate Missions (HPCM), are as follows: Anthropogenic CO<sub>2</sub> monitoring mission (CO<sub>2</sub>M), High Spatio-Temporal Resolution Land Surface Temperature Monitoring Mission (LSTM), Passive Microwave Imaging Mission (CIMR), Hyper Spectral Imaging Mission (CHIME), L-Band SAR Mission (ROSE-L), and the Polar Ice and Snow Topographic Mission (CRISTAL) (ESA Copernicus Website).

### **High-Altitude Pseudo Satellites: HAPS**

ESA is additionally investigating services enabled by High-Altitude Pseudo Satellites (HAPS) complemented by satellites, most recently in a feasibility study completed in September 2019. The latter is supported by EMSA, Satcen, and Frontex, with potential follow-up demonstration projects. Maritime, security, and emergency response services are considered as domains where HAPS can play a key role in the short-term. It is expected that soon users in the civil domain engaged in monitoring and surveillance operations will consider utilization of these assets as a complement to the current data sources, being it space, airborne, or in situ. In this context, the European Maritime Safety Agency (EMSA), Frontex, and the European Union Satellite Centre (SatCen) have expressed their interest to support the current study and will provide requirements and guidance (ESA 2019c).

### **Satellite Communications: SATCOM**

ESA's SATCOM programs consist of the Advanced Research in Telecommunications Systems (ARTES) programs: Future Preparation Phase 6 and Phase 7, Core Competitiveness, ScyLight, ARTES C&G Phase 2, Advanced Technology Phase 2, European Data Relay Satellite System (EDRS), Large Platform, IRIS Phase 2.1 and 2.2, Small Geostationary Satellite (SGEO), Next Generation Platform (NEOSAT), Integrated Applications Promotion (IAP), Satellite Automatic Identification System (AIS) SAT-AIS, Electra, Quantum, ICE, Indigo, ECO, Pioneer, Governmental Satellite Communications (GOVSATCOM) Precursor and Aidan.

### **Secure Satcom for Safety & Security (4S)**

At the ESA Ministerial Council 2019, it was agreed that the Programme of Advanced Research in Telecommunications Systems, ARTES 4.0, as a successor to the ARTES Programme which remains in force, and comprising coordinated but financially autonomous program lines either of a strategic nature or for general purpose, shall be conducted within the framework of the Agency pursuant to the corresponding Declaration entering into force on this day following its subscription by the participating Member States concerned; and NOTES that ARTES 4.0 will provide a streamlined and more responsive programmatic toolset to support industry in the increasingly dynamic and fierce competitive market environment and, reaching beyond telecommunications, will add capabilities and value for other ESA activities and programs (ESA 2019b).

### **GOVSATCOM Precursor Program**

In December 2017, ESA and EDA formalized their cooperation on GOVSATCOM through an Implementing Arrangement. The purpose of this cooperation is to maximize the synergies between the ESA GOVSATCOM Precursor and EDA GOVSATCOM Pooling & Sharing Demonstration. The ESA ARTES program proposal for GOVSATCOM Precursor(s) has been supported at ESA's Ministerial Council in 2016 (CM16) for implementation and in-orbit demonstration during 2017–2020, in preparation of an operational GOVSATCOM program, which is anticipated to be under EC lead (ESA 2017b).

Satellite operators and service providers are developing the first GOVSATCOM precursor public–private partnership projects called PACIS: Pacis 1, Pacis 3, Pacis 5, and Pacis 6. These projects aim to develop secure mission control systems and operations centers and demonstrate the benefits of pooling and sharing to users in the field. The PACIS Projects have been defined as part of a future federation of demonstration projects in the 2017–2020 timeframe. The ESA Govsatcom Precursor program will be implemented in synergy with the Govsatcom Pooling & Sharing Demonstrator that is implemented by the European Defence Agency (EDA). (ESA 2018a).

Additionally, preparations have been initiated for a coherent ARTES programmatic framework for Secure Satcom for Safety & Security (4S) in consistency with the Safety and Security program of ESA for the 2019 ESA Council at ministerial level (ESA 2018a).

### **Remotely Piloted Aircraft Systems: RPAS**

Several ARTES studies relevant to security have been conducted, on certification requirements and performance standards of satellite communication links for RPAS and Air Traffic Services (ATS) as well as in support to emerging System Concepts for Unmanned Aircraft System (UAS) Command and Control via Satellite. Future studies have been prepared to analyze cyber-threats on satellite communication networks and impacts on the global society and to study UHF innovative waveform and satellite communication ground segments (ESA 2017b).

### **ScyLight**

The ARTES ScyLight (Secure and Laser Communication Technology) Element is dedicated to the development and early demonstration of optical communication technology and includes a dedicated programmatic line addressing quantum cryptography technology and Quantum Key Distribution (QKD) missions. The proposals on an ITT for a study on space-based QKD systems to protect Critical European Infrastructures have been evaluated in close coordination with the European Commission's DG GROW and DG CONNECT. Under ScyLight, a first contract on QKD Services was signed on 2 May 2018 about QUARTZ – Quantum Cryptography Telecommunication System between ESA and SES. The project will start with the technology development of a Quantum Key Distribution (ESA 2018a).

Future Air Traffic Management (ATM) will increasingly rely on information sharing based on datalink, requiring a higher level of safety and cyber-security. The ARTES element Iris aims at supplying a validated satellite-based ATM communication solution for Europe. Iris is conducted in close coordination with the Single European Sky ATM Research (SESAR) initiative of the SESAR Joint Undertaking, established as a public-private partnership founded by the European Union and Eurocontrol (ESA [2017b](#)).

### **Positioning, Navigation, and Timing: PNT**

ESA's PNT program consists of the European GNSS Evolution Programme (EGEP) and the Navigation Innovation and Support Programme (NAVISP). Third Party contribution accounts for Galileo Full Operational Capability (FOC), Galileo Deployment Phase, Galileo GSA WA, European Geostationary Navigation Overlay Service (EGNOS) GSA WA, and Horizon 2020.

NAVISP has demonstrated in its first 3 years of implementation its capacity to generate innovative ideas on matters ranging from weather monitoring based on GNSS and sensor data crowdsourcing to the use of pulsars as an independent timescale and of quantum sensing to complement space-based techniques for PNT. During its Phase 2, NAVISP will continue to act along the entire PNT value chain so as to maintain and develop a technological edge beyond the scope of H2020 and future Horizon Europe activities with a view to continuing to support the development of competitive products and services, and thereby generating tangible economic benefits (ESA [2019b](#)).

ESA oversees the implementation of the space infrastructure and R&T preparatory activities for the European GNSS Programme (Galileo and EGNOS) funded by the European Union. The specific high-level security objectives for Galileo are to:

- Ensure the ability of the EU to control the system.
- Ensure the ability for the EU to develop, build, and maintain an independent and autonomous GNSS infrastructure.
- Ensure the ability for the EU to prevent the security issues specific to GNSS infrastructure.

The specific high-level security objectives for EGNOS are to:

- Ensure the ability for the EU to protect the system from malicious or hostile attack that could impact the safe use of the system.
- Ensure the ability of EU to protect any data whose disclosure could adversely affect the ability to provide the EGNOS service (ESA [2017b](#)).

ESA is charged with implementing the security requirements for the program and supports security-related accreditation activities necessary for the correct and successful accreditation by the GNSS Security Accreditation Board (GSAB). The PRS Arrangement between ESA and the European Commission and ESA was under negotiation in 2017. The Arrangement covers:

- The deployment phase of the Galileo program under the EC-ESA Galileo Deployment Delegation Agreement (the agreement lasts until 31st December 2021).
- The exploitation phase of the Galileo program under the European GNSS Agency-ESA Working Arrangement (the agreement is foreseen to last until 31st December 2021).
- The early phases of the evolution of the Galileo program under the EC-ESA Delegation Agreement on the implementation of H2020 Framework Programme.

Parallel to the Galileo FOC deployment completion tasks, potential new or enhanced PRS capabilities are being investigated by ESA as part EC/ESA H2020 Delegation Agreement covering GNSS evolution activities (ESA 2017b).

## **Space Situational Awareness: SSA/Space Surveillance and Tracking – SST**

### **Space Safety Programme (S2P)**

At the ESA Ministerial Council 2019, the Ministers agreed that the Space Safety Programme (S2P), as a successor to the Space Situational Awareness (SSA) Programme, aims to contribute to the protection of Earth, humanity, and assets from hazards originating in space, shall be conducted within the framework of the Agency. S2P will contribute significantly by establishing overall complementarity and maximizing synergies among space safety initiatives in Europe, providing opportunities for cooperation among the Agency, Member States, the European Union and other partners to those ends (ESA 2019b).

The establishment of the Space Safety Programme, in response to increased awareness worldwide of the underlying issues, aims to provide ESA and its Member States with the necessary tools to conduct effective risk management, addressing hazards originating in space through the identification of their different types, the analysis of their status, severity, and magnitude; the prevention of such hazards materializing in the form of genuine threats of damage being caused to Earth or ESA's space infrastructure by activating mitigation measures and providing appropriate information to support Member States activities aimed at ensuring efficient crisis management, thus giving Europe a lead role in the field (ESA 2019b).

The innovative and promising approach offered by the program activities aim at establishing a long-term framework for in-orbit servicing starting with active debris removal performed on an ESA space object, thus offering ESA the opportunity to apply more efficiently in the coming years its policy and guidelines aimed at reducing the harmful effects of space debris and opening up new market opportunities to industry;

Activities related to innovative security and safety applications on Earth in support of European and national policies are also conducted within different optional programs under the Applications pillar (ESA 2019b).

## SSA Programme

ESA's SSA Programme so far has been focusing on three main areas:

- Space Weather (SWE): monitoring and predicting the state of the Sun and the interplanetary and planetary environments, including Earth's magnetosphere, ionosphere, and thermosphere, which can affect spaceborne and ground-based infrastructure thereby endangering human health and safety.
- Near-Earth Objects (NEO): detecting natural objects such as asteroids that can potentially impact Earth and cause damage.
- Space Surveillance and Tracking (SST): watching for active and inactive satellites, discarded launch stages, and fragmentation debris orbiting Earth (ESA 2018d).

ESA's activities in the SST segment focus on the research and development (R&D) for SST data processing techniques, applications, and related standardization of data formats. An effective and efficient exchange between an SST system and external sensors is ensured through researching, developing the technologies, and demonstrating the capabilities of the SST Expert Centers. During Period 2 (2013–2016) of ESA's SSA Programme, these activities integrated the available SST sensors, the simulators within the data processing chain, and the applications, preparing for the SST Core software. The development of an Expert Centre system supporting Laser and Optical tracking technologies and expertise is continuing (ESA 2018d).

Concerning Space Weather (SWE), the SSA Programme has received the mandate to start the development of a SWE mission to L5 (phases A/B), as well as to continue with the implementation of the European SWE system based on a growing number of SWE services. It is also aiming at developing the required SWE instrumentation including magnetographs, radiation monitors, extreme ultraviolet lithography (EUV) imagers, and coronagraph. In the Near-Earth Object (NEO) domain, both the sensors – with the development of the NEO Fly-Eye telescope – and the data and services delivery are addressed, through the deployment of the Near-Earth Objects Dynamic Site (NEODYSS) system in the NEO Coordination Centre at ESRIN (ESA 2017b).

Within the evolving SST landscape in Europe, the SSA Programme is continuing its R&D activities in SST in Period 3, namely, in radar, telescope, and laser system technologies and including providing support to the development of national SST capabilities. It will initiate the development of a space-based optical component for statistical sampling of small-sized debris, to be flown as a hosted payload. It will also develop a community approach to SST core software that will be made available to Participating States for SSA data processing in line with the established SST architecture. The program is also in the process of performing preoperational endurance test and validation activities of the available components of the SST system, including radar and optical sensors, data processing and fusion, correlation, and cataloguing (ESA 2017b).

## North Atlantic Treaty Organization: NATO

### NATO Space and Security Status

NATO was founded in 1949 and has 29 members. Common-funding arrangements principally include the NATO civil and military budgets, as well as the NATO Security Investment Programme (NSIP). NATO's 2019 civil budget was €250.5 million and the military budget €1.395 billion (NATO 2018a).

Space has always been regarded as essential by NATO. NATO relies on space-based services provided by Alliance Nations on a voluntary basis. NATO has a dedicated space policy as of June 2019 and has recognized space as an operational domain alongside air, land, sea, and cyberspace (NATO 2019a, Defense News 2019).

The principal political decision-making body is the North Atlantic Council, which exchanges intelligence, information and other data, compares different perceptions and approaches, harmonizes its views, and takes decisions by consensus, as do all NATO committees. The 2010 NATO Strategic Concept identifies collective defense, crisis management, and cooperative security as the essential core tasks that NATO must continue to fulfil to assure the security of its members. Deterrence based on an appropriate mix of nuclear, conventional, and ballistic missile defense capabilities remains a core element of NATO's overall strategy. The NATO Defence Planning Process is the primary means to identify and prioritize the capabilities required for full-spectrum operations and to promote their development and delivery (NATO Crisis Management).

The NATO Communications and Information (NCI) Agency was established in 2012 as a result of the merger of the NATO Consultation, Command and Control Agency (NC3A), the NATO ACCS Management Agency (NACMA), the NATO Communication and Information Systems Services Agency (NCSA), and the ALTBMD program office and elements of NATO HQ. The NCI Agency delivers secure, coherent, cost effective, and interoperable communications and information systems and services in support of consultation, command & control, and enabling intelligence, surveillance, and reconnaissance capabilities. Within the NCI Agency structure, the Joint Intelligence, Surveillance and Reconnaissance Service Line (JISR SL) is a subelement of the Directorate of Application Services. The NCI Agency operates the Network Control Centre (Mons and Brunssum) which provides service allocation and network monitoring (NCIA Website). The NCI Agency has a vital role in NATO's current space capabilities, supporting in SATCOM, JISR, Navigation Warfare (NAVWAR), and Ballistic Missile Defense (BMD). The BMD Programme, a multi-billion Euro effort, enables NATO nations to act as a single unit when responding to a ballistic missile threat or attack, which requires very quick and coordinated action. The BMD Programme consists of multiple projects that when combined, constitute a capability that connects the entire Alliance to share information and be effective in space, on the ground and at sea (NATO 2019b). Furthermore, The Agency has also participated in the NATO Bi-Strategic Commands' Space Working Group since 2012. The Bi-Strategic Command Space Working Group reports directly to the NATO Military Committee and is committed

to the evolution of space support for alliance military operations. The Space Working Group has been essential for the preparation of the NATO Space Policy and the declaration of space as an operational domain (NITECH 2019).

The Joint Air Power Competence Centre (JAPCC) in Kalkar, Germany, is the NATO Department Head for Space Support to Operations. JAPCC was formed in January 2005 to provide the strategic level proponent for Joint Air and Space (A&S) Power that was missing in NATO. Based on a Memorandum of Understanding, the JAPCC is sponsored by 16 NATO nations (including the UK) who provide a variety of experienced Subject Matter Experts (SME) that come from all three services (JAPCC 2016). Within the JAPCC, a writing team consisting of national experts has been advancing in January 2018 on an update of the 2016 NATO Standard AJP 3.3 Allied Joint Doctrine for Air and Space Operations. JAPCC promotes the full recognition of space as a domain, like land, air, maritime, and cyber domains. JAPCC promotes the complete integration of space in the NATO organization. The areas of NATO space support include: PNT, ISR, SATCOM, METOC (meteorology and oceanography), SEW (Shared Early Warning), and SSA (JAPCC 2016). Within the frame of the actual mandate “NATO’s approach to space – follow-on work,” and as part of the Bi-Strategic Command Space Working Group, JAPCC contributed to the production of a “NATO Overarching Space Policy (OSP)” that was published in June 2019. JAPCC contributed to an advice paper for the International Military Staff (IMS) that led to a declaration in December 2019 that NATO recognizes Space as an operational domain (JAPCC 2019b). Additionally, JAPCC is involved in the 2-year-long Science and Technology Organization (STO) project as an active contributor. Today, space-related data and products from different NATO nations include variations in data protocols and sensor attributes (JAPCC 2019b).

The NATO Support and Procurement Agency (NSPA) provides follow-on logistic support for NATO-funded and non-NATO-funded communication and information systems. These include SATCOM Satellite Ground Terminals (SGT), Transportable SGTs (TSGT), and Man-Packs. The services provided by NSPA cover: Supply from central and distributed stocks; Centralized/consolidated procurement of parts; Direct Exchange (DX); Depot Level Maintenance (DLM); Technical/engineering services; and Transportation (NSPA Website).

## **NATO Space and Security Activities/Programs**

### **Earth Observation: EO/Intelligence, Surveillance, and Reconnaissance – ISR**

Under the NATO Civilian Structure, in the NATO Air Force Armaments Group and within the Defence Investment Division, there is a dedicated Joint Capability Group Intelligence, Surveillance, and Reconnaissance (NATO Organization).

With the frame of NATO Capabilities, Joint Intelligence, Surveillance and Reconnaissance (JISR) is considered crucial. JISR brings together data and information gathered through projects such as NATO’s Alliance Ground Surveillance (AGS) system or NATO AWACS aircraft as well as a wide variety of national JISR assets from the space, air, land, and maritime domains. NATO’s use of space-based

ISR is centered on the following elements: Intelligence: the final product derived from surveillance and reconnaissance, fused with other information; Surveillance: the persistent monitoring of a target; and Reconnaissance: information-gathering conducted to answer a specific military question (NATO 2018b).

NATO has a German-led smart defense initiative called Multinational Geospatial Support Group (GSG). The GSG provides enhanced standardized geospatial information, such as mapping and terrain imaging to NATO operations and planning (geospatial operational support, data management, terrain analysis, reproduction capability through maps and digital products, in theatre data collection). The following members are included in the GSG: Canada, Czech Republic, Germany, Denmark, Spain, France, UK, Greece, The Netherlands, Norway, Poland, Romania, and Turkey. Italy, Austria, Finland, Croatia, and the USA are considering membership (NATO 2014a).

JISR brings together data and information gathered through projects such as NATO's Alliance Ground Surveillance (AGS) system or NATO Airborne Warning & Control System (AWACS) surveillance aircraft as well as a wide variety of national JISR assets from the space, air, land, and maritime domains (NATO 2018b). The NATO AGS is acquired by 15 Allies (Bulgaria, Czech Republic, Denmark, Estonia, Germany, Italy, Latvia, Lithuania, Luxembourg, Norway, Poland, Romania, Slovakia, Slovenia, and the United States). All NATO Allies contribute to the development of the AGS capability through financial contributions covering the establishment of the AGS main operating base, as well as to communications and life-cycle support of the AGS fleet. Some Allies replace part of their financial contribution through interoperable contributions in kind (national surveillance systems that will be made available to NATO). The NATO-owned and NATO-operated AGS Core capability will enable the Alliance to perform persistent surveillance over wide areas from high-altitude, long-endurance (HALE) aircraft, operating at considerable stand-off distances and in any weather or light condition. Using advanced radar sensors, these systems will continuously detect and track moving objects throughout observed areas and will provide radar imagery of areas of interest and stationary objects. The Main Operating Base for AGS is located at Sigonella Air Base in Italy, which will serve a dual purpose as a NATO JISR deployment base and data exploitation and training center (NATO 2017).

The air segment consists of five RQ-4B Global Hawk Block 40 aircraft and remotely piloted aircraft (RPA) flight control element. The aircraft will be equipped with a state-of-the-art, multi-platform radar technology insertion program (MP-RTIP) ground surveillance radar sensor, as well as an extensive suite of line-of-sight and beyond-line-of-sight, long-range, wideband data links. The ground segment will provide an interface between the AGS Core system and a wide range of command, control, intelligence, surveillance, and reconnaissance (C2ISR) systems to interconnect with and provide data to multiple deployed and non-deployed operational users, including reach-back facilities remote from the surveillance area. The ground segment consists of several ground stations in various configurations, such as mobile and transportable, which will provide data-link connectivity, data-processing, and exploitation capabilities and interfaces for interoperability with C2ISR systems (NATO 2017).



## Satellite Communications: SATCOM

NATO use of Satellite Communications (SATCOM) is centered on the following uses:

- Command, Control and Communications (C3) Systems
- Remotely Piloted Aircraft Systems (RPAS) operations
- Beyond Line-Of-Sight (BLOS) communications (NATO 2017)

On February 12, 2020, NATO concluded a Memorandum of Understanding between four nations for the provision of critical satellite communications services to NATO for the next 15 years. The memorandum between France, Italy, the United Kingdom, and the United States enables the four Allies to provide space capacity from their military satellite communications (SATCOM) programmers to NATO. Nations began delivering the capability on 1 January 2020 (NATO 2020). In 2019, NATO authorized 1 €billion for satellite SATCOM services for the next 15 years. The NCI Agency is responsible for operating the satellite communications capability to deliver services to NATO.

NATO has owned a series of military communication satellites, encrypted for use by NATO and designed to link the capital cities of NATO countries. NATO-1 and -2 were launched in 1970 and 1971, respectively, and four of the much larger NATO-3 satellites between 1976 and 1984. Each NATO-3 could support hundreds of users and provide voice and facsimile services in UHF- (ultra-high frequency), X-, and C-bands (see frequency bands). Two NATO-4 satellites, which operate in the same bands but have still more channels, were launched in 1991 and 1993. NATO does not today own any on orbit spacecraft but does own and operate several terrestrial elements such as SATCOM anchor stations and terminals (NATO 2016).

Since 2005, NATO has been making use of Member States' capacities, dealing with core strategic communications and services from the private sector. The C2 for SATCOM is managed by NATO Communication and Information Agency (NCIA) and operated by NATO CIS Group (NATO 2016). Concerning effective C2, the concept of Multi-Domain Operations (MDO) is used to "converge air, space, and cyber capabilities to meet the challenges of these contested domains." Accordingly, "space superiority is the number one priority. NATO won't necessarily win the war with it but losing in space virtually guarantees that NATO will lose it" (JAPCC 2019a).

Under the current NATO SATCOM Post-2000 (NSP2K) program – SATCOM Capability Package CP5A0030 – a consortium formed by the British, French, and Italian governments provide NATO with advanced SATCOM capabilities for a 15-year period from January 2005 until the end of 2019. Under a memorandum of understanding, the program provided NATO with access to the military segments of three national satellite communications systems – the French SYRACUSE 3, the Italian SICRAL 1 and 1Bis, and the British Skynet 4 and 5. This satellite capability has replaced the two NATO-owned and NATO-operated NATO IV communications satellites, which stopped their operational services in 2007 and 2010, respectively, after a combined operational life of 19 years. The SYRACUSE, SICRAL, and Skynet 4/5 satellites provided Super High Frequency (SHF) communications with

military hardening features, while Ultra High Frequency (UHF) communications were provided by the SICRAL and Skynet satellites (NATO 2011). The NSP2K agreement was terminated at the end 2019.

As, the NSP2K came to an end, NATO has addressed the Follow-up Capability Package (CP9A0130) or CP130 which begins in 2020. CP9A0130 provides: SHF, UHF, and Extremely high frequency (EHF) space segment capabilities for 2019–2034, and ground and control segment capabilities such as new and/or upgrades for ground terminals, modems, and network control (NATO 2014b). With the funding approval pending, the planned 15-year €1.5billion CP130 will be devoted to upgrading the space segment and improve the ground segment. The objective is that the third-generation transportable satellite ground terminals will be upgraded, and the new fourth-generation terminals will be purchased. The current consortium of nations will be expanded to include the US, while contingency arrangements will be put in place with commercial providers in order to meet urgent requirements (NITECH 2019).

### **Positioning, Navigation, and Timing: PNT**

NATO operations rely significantly on space support services given by the member nations. One of the most essential is the Positioning, Navigation, and Timing (PNT) service, provided by the United States’.

Global Positioning System (GPS) constellation (NATO 2017). NATO’s use of space-based PNT addresses the following uses (NATO 2017):

- Precision strike
- Force navigation movements
- Logistic support
- Network timing
- Navigation Warfare (NAVWAR)
- Land and coastlines accurate survey
- Countering Improvised Explosive Devices (C-IED)
- Ballistic missile warning and defeat
- Cryptographic support (key generation)

According to JAPCC, military receivers rely on protected signals. In the case of GPS, the military uses the Precise Positioning Service (PPS), based on the so-called P(Y) code, which can use two different frequencies. Galileo is protected by the Public Regulated Service (PRS) and uses two frequencies as well, different from the GPS frequencies. NATO’s threat assessment concludes that a combination of GPS and Galileo will increase the jamming resistance. An opponent will either opt for more jammers to affect the additional frequencies or concentrate on specific geographic areas or sectors to jam PNT signals (JAPCC 2019d).

NATO’s ongoing work in the field of PNT is carried out within the NATO Command, Control and Consultation Board (NC3B). This board is organized into capability panels (CaP). CaP “Identification and Navigation” includes various Capability Teams such as NAVWAR, Interface Standardization between receivers, and PNT relevance for air space procedures (NATO 2017).

### **Space Situational Awareness: SSA/Space Surveillance and Tracking (SST)**

NATO reliance on Space Situational Awareness (SSA) services is based on the voluntary contribution of allied nations (JAPCC 2016). NATO use of SSA addresses (NATO 2017):

- Space assets defense, including notification of potential collisions with Space debris
- Surveillance of Space
- Prevention of an adversary's ability to use Space systems and services for purposes hostile to a Nation's security interests

JAPCC 2019 White Paper "Command and Control of a Multinational Space Surveillance and Tracking Network" provides a NATO perspective on emerging multinational SST endeavors. It emphasizes the advantages of an EU SST network for the alliance and promotes the importance of Space Situational Awareness and SST in support of NATO military operations. The White Paper mentions that "since national SST resources often include a significant percentage of military assets, a serious multinational governmental SST endeavor cannot exclude the national Ministries of Defence." It adds: "from a military perspective, this situation is a source of both concerns and opportunities. In one sense, it raises concerns about the opportunity of sharing classified data regarding military spacecraft (own or allied). Additionally, since SST is often a secondary task for most military sensors, nations should carefully consider their level of commitment to SST because it drains resources from their primary task, usually airspace control or missile warning" (JAPCC 2019c).

---

## **Conclusion**

Security and defense policies are progressively and gradually being supported by space programs of institutions in Europe. In Europe, the European Union and the European Space Agency are the main players together with their Member States. The various space subdomains they get involved in are notably, Earth observation; SATCOM; and Positioning, Navigation, and Timing. The European Defense Agency and the European Union Satellite Center follow suit in space programs for security and defense purposes, with an increasing interest by NATO. Yet, the Ministries of Defence in the Member States have a central role in the decision-making related to space and security in these organizations. The different nature and purpose of each organization leads to diversified development of activities and programs. In addition, whereas civil and defense space activities mainly comprise separate programs, more and more new programs follow a dual-use approach, right from their conception. This means that both civil as well as military funding may contribute in funding the same program. Additionally, both civil and military user communities are envisaged for specific space assets and applications. These

developments in space programs frame to an increasing extent the necessity of Europe to take its security and defense at the next level by incorporating existing assets and jointly building new ones.

**Disclaimer** The contents of this Chapter and any contributions to the Handbook reflect personal opinions and do not necessarily reflect the opinion of the European Space Agency (ESA).

---

## References

- Copernicus Website, About Copernicus. Available at: <https://www.copernicus.eu/en/about-copernicus/copernicus-brief>
- Council of the EU (2014) Decision 2014/401/CFSP of 26 June 2014 on the European Union Satellite Centre and repealing Joint Action 2001/555/CFSP on the establishment of a European Union Satellite Centre, 27 June 2014. Available at: <http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014D0401&from=GA>
- Council of the EU (2018) Council of the European Union, Report from the Commission to the European Parliament and the Council on the implementation of the Space Surveillance and Tracking (SST) support framework (2014–2017), 8891/18, 18 May 2018, Brussels. Available at: <http://data.consilium.europa.eu/doc/document/ST-8891-2018-INIT/en/pdf>
- Council of the EU (2019a) Frontex draft Programming Document 2020–2022, 20 November 2019, Brussels. Available at: <https://data.consilium.europa.eu/doc/document/ST-14362-2019-INIT/en/pdf>
- Council of the EU (2019b) Promoting synergies between the EU civil and military capability development – European space situational awareness high level civil-military user requirements document, 15715/11, 24 October 2011. Brussels
- Defense News (2019) NATO names space as an ‘operational domain,’ but without plans to weaponize it, 20 November 2019. Available at: <https://www.defensenews.com/smr/nato-2020-defined/2019/11/20/nato-names-space-as-an-operational-domain-but-without-plans-to-weaponize-it/>
- EDA (2016a) European Defence agency, persistent surveillance long term analysis (SULTAN), 19 January 2016. Available at: [https://www.eda.europa.eu/what-we-do/activities/activities-search/persistent-surveillance-long-term-analysis-\(sultan\)](https://www.eda.europa.eu/what-we-do/activities/activities-search/persistent-surveillance-long-term-analysis-(sultan))
- EDA (2016b) European Defence Agency, Towards Enhanced European Future Military Capabilities, European Defence Agency Role in Research & Technology:2016. Available at: <https://www.eda.europa.eu/docs/default-source/eda-publications/eda-r-t-2016-a4%2D%2D-v09>
- EDA (2017a) European Defence agency, three questions to Pascal Legai – director of the EU satellite Centre (SatCen). EDM 13:2017. Available at: <https://eda.europa.eu/docs/default-source/eda-magazine/edmissue13lowresweb.pdf>
- EDA (2017b) European Defence agency, REACT: EDA study to boost imagery intelligence. EDM 13:2017. Available at: <https://eda.europa.eu/docs/default-source/eda-magazine/edmissue13lowresweb.pdf>
- EDA (2017c) European Defence agency, governmental satellite communications, fact sheet, 16 June 2017. Available at: [https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-06-16-factsheet\\_govsatcom](https://www.eda.europa.eu/docs/default-source/eda-factsheets/2017-06-16-factsheet_govsatcom)
- EDA (2018a) European Defence agency, capability development plan, June 2018. Available at: <https://www.eda.europa.eu/what-we-do/our-current-priorities/capability-development-plan>
- EDA (2018b) European Defence agency, chief executive Domecq at ESA, 5 February 2018, <https://eda.europa.eu/info-hub/press-centre/latest-news/2018/02/05/chief-executive-domecq-at-esa>
- EDA (2018c) European Defence agency, information sheet on space, 21 September 2018, <https://www.eda.europa.eu/docs/default-source/documents/eda-information-sheet-on-space.pdf>

- EDA (2020a) European Defence agency, factsheet: EU SatCom market, 4 February 2020. Available at: <https://www.eda.europa.eu/info-hub/publications/publication-details/pub/factsheet-eu-satcom-market>
- EDA (2020b) European Defence Agency, ESA and EDA joint research: advancing into the unknown, 9 January 2020. Available at: <https://www.eda.europa.eu/info-hub/publications/publication-details/pub/factsheet-eu-satcom-market>
- EDA PESCO (2018) European Defence Agency, Current list of PESCO projects. Available at: [https://www.eda.europa.eu/what-we-do/our-current-priorities/permanent-structured-cooperation-\(PESCO\)/current-list-of-pesco-projects](https://www.eda.europa.eu/what-we-do/our-current-priorities/permanent-structured-cooperation-(PESCO)/current-list-of-pesco-projects)
- ESA (2016) Joint Statement on Shared Vision and Goals for the Future of Europe in Space by the EU and ESA, 26 October 2016. Available at: [http://www.esa.int/About\\_Us/Welcome\\_to\\_ESA/Shared\\_vision\\_and\\_goals\\_for\\_the\\_future\\_of\\_Europe\\_in\\_space](http://www.esa.int/About_Us/Welcome_to_ESA/Shared_vision_and_goals_for_the_future_of_Europe_in_space)
- ESA (2017a) European Space Agency, Europe's master plan for space technology by ESA and the EU, 20 December 2017
- ESA (2017b) European Space Agency, Status Report on ESA's security related developments and activities, ESA/C (2017)62, June 2017, Paris
- ESA (2017c) European Space Agency, Space-based Services in Support of CBRNe Operations, Feasibility Study, May–August 2017. Available at: <https://business.esa.int/funding/invitation-to-tender/space-based-services-support-cbrne-operations>
- ESA (2018a) European Space Agency, Status Report on ESA's Safety and Security-Related Developments and Activities, ESA/C(2018)58, 29 May 2018, Paris
- ESA (2018b) European Space Agency, The Contribution of ESA to Copernicus 2.0, ESA/PB-EO (2018)8, 2 February 2018, Paris
- ESA (2018c) European Space Agency, Copernicus evolution – Copernicus Space Component (CSC) Long Term Scenario (LTS), 9 May 2018, ESA/PB-EO (2018)12. France, Paris
- ESA (2018d) European Space Agency, laser-tracking and optical expert Centre status and first results, ESA/PB-SSA(2018)16, 16 May 2018. France, Paris
- ESA (2018e) European Space Agency, draft amendment no 5 to the Galileo deployment delegation agreement between ESA and the EU, ESA/AF(2018)11, 7 February 2018, Paris
- ESA (2019a) European Space Agency, N° 22–2019: ESA ministers commit to biggest ever budget, 28 November 2019. Available at: [https://www.esa.int/Newsroom/Press\\_Releases/ESA\\_ministers\\_commit\\_to\\_biggest\\_ever\\_budget](https://www.esa.int/Newsroom/Press_Releases/ESA_ministers_commit_to_biggest_ever_budget)
- ESA (2019b) European Space Agency, Resolution on ESA programs: addressing the challenges ahead, adopted on 28 November 2019, ESA/C-M/CCLXXXVI/Res.3. Available at: [https://www.esa.int/Newsroom/Press\\_Releases/ESA\\_ministers\\_commit\\_to\\_biggest\\_ever\\_budget](https://www.esa.int/Newsroom/Press_Releases/ESA_ministers_commit_to_biggest_ever_budget)
- ESA (2019c) European Space Agency, Services enabled by HAPS – Services enabled by High Altitude Pseudo Satellites (HAPS) complemented by satellites. Available at: <https://business.esa.int/projects/services-enabled-haps>
- ESA (2019d) European space agency, new financial resources for Copernicus space component, 22 January 2019. Available at: [https://www.esa.int/Applications/Observing\\_the\\_Earth/Copernicus/New\\_financial\\_resources\\_for\\_Copernicus\\_space\\_component](https://www.esa.int/Applications/Observing_the_Earth/Copernicus/New_financial_resources_for_Copernicus_space_component)
- ESA Ariane 6, European Space Agency, Ariane 6. Available at: [https://www.esa.int/Enabling\\_Support/Space\\_Transportation/Launch\\_vehicles/Ariane\\_6](https://www.esa.int/Enabling_Support/Space_Transportation/Launch_vehicles/Ariane_6)
- ESA Copernicus Website, Space Component overview. Available at: [https://www.esa.int/Applications/Observing\\_the\\_Earth/Copernicus/Space\\_Component](https://www.esa.int/Applications/Observing_the_Earth/Copernicus/Space_Component)
- European Commission (2018a) Press release, EU budget: a €16 billion space Programme to boost EU space leadership beyond 2020, Brussels, 6 June 2018
- European Commission (2018b) Proposal for a Regulation of the European Parliament and of the Council Establishing the Space Policy Programme of the European Union, Relating to the European Union Agency for Space and Repealing Regulations (EU). No 1285/2013, No 377/2014 and No 912/2010 and Decision 541/2014/EU, COM (2018) 447 final 2018/0236 (COD), 6 June 2018, Brussels. Available at: [https://ec.europa.eu/commission/sites/beta-political/files/budget-june2018-space-programme-regulation\\_en.pdf](https://ec.europa.eu/commission/sites/beta-political/files/budget-june2018-space-programme-regulation_en.pdf)

- European Commission (2019a) Orientations towards the first strategic plan implementing the research and innovation framework Programme horizon Europe, Co-design via web open consultation, summer 2019. Available at: [https://ec.europa.eu/research/pdf/horizon-europe/ec\\_rtd\\_orientations-towards-the-strategic-planning.pdf](https://ec.europa.eu/research/pdf/horizon-europe/ec_rtd_orientations-towards-the-strategic-planning.pdf)
- European Commission (2019b) The future is quantum: EU countries plan ultra-secure communication network, 13 June 2019. Available at: <https://ec.europa.eu/digital-single-market/en/news/future-quantum-eu-countries-plan-ultra-secure-communication-network>
- European Commission, DG GROW Website, internal market, industry, Entrepreneurship and SMEs Available at: [https://ec.europa.eu/growth/about-us\\_en](https://ec.europa.eu/growth/about-us_en)
- European Commission, Galileo Website. Available at: [https://ec.europa.eu/growth/sectors/space/galileo\\_en](https://ec.europa.eu/growth/sectors/space/galileo_en)
- European Council (2013) Conclusions, EUCO 217/13, 20 December 2013, Brussels. Available at: <http://data.consilium.europa.eu/doc/document/ST-217-2013-INIT/en/pdf>
- European Parliament (2014) Decision no 541/2014/EU of the European Parliament and of the council of 16 April 2014 establishing a framework for space surveillance and tracking support OJ L 158, 27 May 2014
- European Parliament (2018) Parliamentary questions, E-006244/2016, answer given by Ms Bieńkowska on behalf of the commission, 18 January 2018. Available at: <http://www.europarl.europa.eu/sides/getAllAnswers.do?reference=E-2016-006244&language=EN>
- EUSST Website, EU SST Support Framework, EU SST Governance. Available at: <https://www.eusst.eu/project/who-we-are/>
- Giannopapa C, Adriaensen M, Antoni N, Schrogl K-U (2018) Elements of ESA's policy on space and security. *Acta Astronautica* 147:346–349
- GPS World (2018) Galileo ground segment keeps constellation on track, 28 March 2018. Available at: [https://www.gpsworld.com/galileo-ground-segment-keeps-constellation-on-track/?utm\\_source=gps\\_navigate&utm\\_medium=email&utm\\_campaign=gps\\_navigate\\_04032018&eid=376813635&bid=2055906;utm\\_source=gps\\_navigate&utm\\_medium=email&utm\\_campaign=gps\\_navigate\\_04032018&eid=376813635&bid=2055906](https://www.gpsworld.com/galileo-ground-segment-keeps-constellation-on-track/?utm_source=gps_navigate&utm_medium=email&utm_campaign=gps_navigate_04032018&eid=376813635&bid=2055906;utm_source=gps_navigate&utm_medium=email&utm_campaign=gps_navigate_04032018&eid=376813635&bid=2055906)
- GSA (2017) EGNOS Open Service (OS) Service Definition Document, 2017. Available at: [https://www.gsa.europa.eu/sites/default/files/brochure\\_os\\_2017\\_v6.pdf](https://www.gsa.europa.eu/sites/default/files/brochure_os_2017_v6.pdf)
- GSA (2020) Space is an enabler of security and defense, 7 February 2020. Available at: <https://www.gsa.europa.eu/newsroom/news/space-enabler-security-and-defence>
- JAPCC (2016) Joint Air Power Competence Centre, Multinational Space Surveillance and Tracking Initiatives from a NATO Perspective. Available at: <https://www.japcc.org/looking-up-together-multinational-space-surveillance-tracking-initiatives-nato-perspective/>
- JAPCC (2019a) Joint air power competence Centre, Joint air & Space Power Conference 2019, Shaping NATO for multi-domain Operations of the future. Multi-Domain Operations and Counter-Space, By Major Richard W. Gibson. Available at: <https://www.japcc.org/what-is-a-multi-domain-operation/>
- JAPCC (2019b) Joint air power competence Centre, Annual Report 2019. Available at: [https://www.japcc.org/wp-content/uploads/JAPCC\\_AR\\_2019\\_screen.pdf](https://www.japcc.org/wp-content/uploads/JAPCC_AR_2019_screen.pdf)
- JAPCC (2019c) Joint air power competence Centre, command and control of a multinational space surveillance and tracking network, June 2019. Available at: [https://www.japcc.org/wp-content/uploads/JAPCC\\_C2SST\\_2019\\_screen.pdf](https://www.japcc.org/wp-content/uploads/JAPCC_C2SST_2019_screen.pdf)
- JAPCC (2019d) Joint air power competence Centre, is NATO ready for Galileo? How the combination of GPS and Galileo could increase NATO's resiliency in PNT, June 2019. Available at: <https://www.japcc.org/is-nato-ready-for-galileo/>
- NATO (2011) SATCOM Post-2000 – Improved satellite communications for NATO, last updated 15 December 2011. Available at: [https://www.nato.int/cps/en/natohq/topics\\_50092.htm](https://www.nato.int/cps/en/natohq/topics_50092.htm)
- NATO (2014a) NATO, Multinational Geospatial Support Group, information flyer, JUNE 2014
- NATO (2014b) NCIA Exploring the Future for NATO Communications Capabilities NATO, Communications Services (NCS) Roadmaps. Available at: <http://citeseerx.ist.psu.edu/>

- [viewdoc/download;jsessionid=9F8558DA0CB4D5C0A9043E7189DFDD17?doi=10.1.1.663.3478&rep=rep1&type=pdf](#)
- NATO (2016) NATO standard AJP-3.3 – Allied Joint Doctrine for Air and Space Operations, Edition B version 1, April 2016. Available at: [https://www.gov.uk/government/uploads/system/uploads/attachment\\_data/file/624137/doctrine\\_nato\\_air\\_space\\_ops\\_ajp\\_3\\_3.pdf](https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/624137/doctrine_nato_air_space_ops_ajp_3_3.pdf)
- NATO (2017) The key role of space support in NATO Operations, Three Swords Magazine, 32/2017, July 2017. Available at: [http://www.jwc.nato.int/images/stories/\\_news\\_items\\_/2017/SPACESUPPORT\\_NATO\\_ThreeSwordsJuly17.pdf](http://www.jwc.nato.int/images/stories/_news_items_/2017/SPACESUPPORT_NATO_ThreeSwordsJuly17.pdf)
- NATO (2018a) NATO agrees 2019 civil and military budgets for further adaptation, December 2018. Available at: [https://www.nato.int/cps/en/natohq/news\\_161633.htm?selectedLocale=en](https://www.nato.int/cps/en/natohq/news_161633.htm?selectedLocale=en)
- NATO (2018b) Joint Intelligence, Surveillance and Reconnaissance, June 2018. Available at: [https://www.nato.int/cps/en/natohq/topics\\_111830.htm](https://www.nato.int/cps/en/natohq/topics_111830.htm)
- NATO (2019a) Foreign ministers take decisions to adapt NATO, recognize space as an operational domain, 20 November 2019. Available at: [https://www.nato.int/cps/en/natohq/news\\_171028.htm](https://www.nato.int/cps/en/natohq/news_171028.htm)
- NATO (2019b) NATO's ballistic missile Defence Programme gets a makeover, 25 November 2019. Available at: [https://www.nato.int/cps/en/natohq/news\\_171028.htm](https://www.nato.int/cps/en/natohq/news_171028.htm)
- NATO (2020) NATO begins using enhanced satellite services, 12 February 2020. Available at: <https://www.ncia.nato.int/NewsRoom/Pages/20200212-NATO-begins-using-enhanced-satellite-services.aspx>
- NATO Crisis Management. Available at: [https://www.nato.int/cps/en/natohq/topics\\_49192.htm](https://www.nato.int/cps/en/natohq/topics_49192.htm)
- NATO, NATO Organization. Available at: <https://www.nato.int/cps/su/natohq/structure.htm>
- NCIA Website, NATO Communications and Information Agency, Joint Intelligence, Surveillance and Reconnaissance. Available at: <https://www.ncia.nato.int/Our-Work/Pages/Joint-Intelligence-Surveillance-and-Reconnaissance.aspx>
- NITECH (2019) NATO innovation and technology, issue 2, October 2019. Available at: [https://issuu.com/globalmediapartners/docs/nitech\\_issue\\_02\\_oct\\_2019?fr=sNjc5YTMyNjE3NQ](https://issuu.com/globalmediapartners/docs/nitech_issue_02_oct_2019?fr=sNjc5YTMyNjE3NQ)
- NSPA Website, NATO Support and Procurement Agency, Satellite Communication Systems. Available at: <https://www.nspa.nato.int/en/organization/Logistics/WSES/satellite.htm>
- Satcen (2016) EU Satellite Centre Annual Report:2016. Available at: [https://www.satcen.europa.eu/key\\_documents/EU%20SatCen%20Annual%20Report%20201658e24cb1f9d7202538bed52b.pdf](https://www.satcen.europa.eu/key_documents/EU%20SatCen%20Annual%20Report%20201658e24cb1f9d7202538bed52b.pdf)
- Schrogl K-U et al (eds) (2015) Handbook of space security: policies, applications and programs. Springer, New York
- Sitruk A, Plattard S (2017) The Governance of Galileo, ESPI Report 62, January 2017. Available at: [https://www.espi.or.at/images/Rep62\\_online\\_170203\\_1142.pdf](https://www.espi.or.at/images/Rep62_online_170203_1142.pdf)



# Space and Security Programs in the Largest European Countries

# 62

Ntorina Antoni, Christina Giannopapa, and Maarten Adriaensen

## Contents

Introduction .....	1226
France .....	1227
Space and Security Budget .....	1227
Space and Security Activities and Programs .....	1227
Germany .....	1237
Space and Security Budget .....	1237
Space and Security Activities and Programs .....	1237
Italy .....	1243
Space and Security Budget .....	1243
Space and Security Activities and Programs .....	1244
Spain .....	1248
Space and Security Budget .....	1248
Space and Security Activities and Programs .....	1248
The United Kingdom .....	1252
Space and Security Budget .....	1252
Space and Security Activities and Programs .....	1252
Concluding Remarks .....	1256
References .....	1257

---

N. Antoni (✉)

Eindhoven University of Technology, Eindhoven, The Netherlands

e-mail: [ntorina.antoni@gmail.com](mailto:ntorina.antoni@gmail.com)

C. Giannopapa · M. Adriaensen

European Space Agency (ESA), Paris, France

e-mail: [christina.giannopapa@esa.int](mailto:christina.giannopapa@esa.int); [maarten.cm.adriaensen@gmail.com](mailto:maarten.cm.adriaensen@gmail.com)



---

**Abstract**

This chapter presents space and security programs in the five largest European countries and indicates their main priorities and trends. Recent policy developments in European countries, this have influenced national and institutional space security programs. The current chapter addresses different types of space activities and programs in the fields of Earth observation (EO), Intelligence-Surveillance-Reconnaissance (ISR), Satellite communication (SATCOM), positioning, navigation, and timing (PNT), and Space Situational Awareness (SSA). The countries presented are France, Germany, Italy, Spain, and the United Kingdom (UK).

---

**Introduction**

The increased need for security in Europe and for Europe's space activities has led to several activities and programs developed in aerospace and defense. The main actors in Europe engaging in space and security activities are the European countries, the European Union (EU), and the European Space Agency (ESA). ► [Chap. 61, "Institutional Space Security Programs in Europe"](#) describes how security and defense policies are progressively and gradually being supported by space programs of the EU and ESA, while the North Atlantic Treaty Organization (NATO) is also gradually involved. The European countries' space security policies are to a large extent determined by national needs and priorities, as explained in ► [Chap. 25, "Space and Security Policy in Selected European Countries."](#) In addition, the policies are influenced by the overall space and security governance and their participation in relevant organizations as explained in ► [Chap. 23, "Strategic Overview of European Space and Security Governance."](#)

The current chapter addresses space and security budgets, activities, and programs of selected European countries in the fields of Earth observation (EO), Intelligence-Surveillance-Reconnaissance (ISR), Satellite communication (SATCOM), positioning, navigation, and timing (PNT), and Space Situational Awareness (SSA). European countries may be distinguished not only on the basis of their membership to space and security related organizations but also their space budget. In the absence of an official grouping, their ESA annual budget and their defense expenditure as a share of their Growth Domestic Product (GDP) are used for their classification (Sagath et al. 2018).

The group presented in this chapter includes ESA Member States with a GDP above €1.2 trillion and an annual ESA space budget (2018 ESA budget) above €200 million: France, Germany, Italy, Spain, and the UK (Sagath et al. 2018). This chapter complements the chapters on medium-size and smaller European countries presented in this section of the handbook. The content is up to date until January 2019.

## France

### Space and Security Budget

France had an estimated defense expenditure of €42.748 billion or 1.84% of GDP in 2018, below the NATO guideline of 2% of GDP. 24.4% of the 2018 defense budget was allocated to equipment expenditure (NATO 2019). The Bill on Military Planning 2019–2025 foresees an expenditure of €295 billion on defense for the period 2019–2025 (French Republic 2018b; RTL INFO 2018). The French Senate adopted on 29 May 2018 the Military Program Law (*Loi de Programmation Militaire - LPM*) 2019–2025 on military funding program. The LPM 2019–2025 aims to renew the French armed forces and end decades of falling defense spending to reach NATO's guideline of 2% of GDP by 2025, according to the French Ministry of the Armed Forces. The final text of the LMP 2019–2025 was agreed by a joint committee of the National Assembly and Senate (Le Figaro 2018). President Macron formally signed the LPM on 13 July 2018. The French Senate and lower house National Assembly had previously examined the draft law, and both had voted in favor of the bill. One of the amendments added to the bill was an annual parliamentary review of spending (Defence News 2018a).

French government expenditure for space-related activities is the largest in Europe. It amounted to €2.8 billion in 2018, of which €2.23 billion covered civil activities and €569 million defense activities (Euroconsult 2019). French Space Agency - CNES's budget for the national program amounted to €1.2 billion in 2018, financed by the Ministry of Research to support innovation and competitiveness. The civil space budget is divided between the national program (€1.187 billion in 2018) and the contributions to ESA (€963 million) and to EUMETSAT (€84 million). The defense budget fluctuates according to procurement cycles. Telecommunication was the primary application in 2018 for the development of Syracuse IV. The Military Program Law plans €3.6 billion investment over 2019–2025 to replace the current systems and acquire electronic intelligence capacity (Euroconsult 2019). Defense space expenditure was estimated at €569 million in 2018, primarily channeled toward telecommunications, Earth observation, technology, and space security. In 2018 the Ministry of the Armed Forces allocated €60 million for the CERES (*Capacité de Renseignement Électromagnétique Spatiale*) military electronic intelligence mission (Euroconsult 2019).

### Space and Security Activities and Programs

#### Earth Observation (EO): Intelligence-Surveillance-Reconnaissance (ISR)

The civilian satellite *SPOT 1- Systeme Probatoire d'Observation de la Terre* (Probative System for Earth Observation) was developed and launched under the responsibility of scientific staff from CNES (Schrogl et al. 2015). The dissemination of information was allocated to the company Spot Image, which was created to

distribute the images of SPOT. SPOT 4 was launched in March 1998 from Kourou. It featured two imaging instruments offering panchromatic and multispectral acquisition mode. SPOT 4 stopped functioning in July 2013. SPOT 5 was launched on 4 May 2002 from Kourou and stopped functioning in March 2015 (Schrogl et al. 2015). SPOT 6, launched in December 2012, and SPOT 7, launched in June 2014, share orbits with Pléiades. The SPOT satellites are dual-use civilian satellites, related to military programs. The United States (US) military has been a major purchaser of SPOT series commercial imagery. SPOT has been transferred to Airbus Defence and Space for operations and development of replacement capabilities (Schrogl et al. 2015).

*Hélios* is a French optical satellite imaging constellation for military reconnaissance. The *Hélios-1* program was the result of a cooperation of France with Italy, and Spain. The first-generation *Hélios* satellites, *Hélios 1A* and *1B*, were launched in 1995 and 1999. Featuring daily revisit capability, the satellites had a resolution of about 1 meter (IAI 2003). The *Hélios* program was expected to reach a new phase with the joint development of *Hélios-2* by France and *Horus* by Germany: *Hélios* in the optical field and *Horus* in that of radar. Due to political and budgetary difficulties in Germany, the project remained on a national level. France consequently decided to pursue the *Hélios-2* program alone with fitting in bilateral cooperation along the way (IAI 2003). The second-generation of the program began with the launch of *Hélios 2A* on 18 December 2004. *Hélios 2B* was launched on 18 December 2009. *Hélios 2B* is managed by the French procurement agency *Direction générale de l'armement (DGA)*. DGA has delegated the responsibility for the space segment to CNES. The *Hélios-2* satellites – *H-2A* and *H-2B* – provide defense users with high-resolution imagery from low Earth orbit (LEO). *Hélios-2* is a cooperation program of France with Belgium, Spain, Greece as co-owners, and Italy and Germany via exchange of data. *Hélios-2* is the only fully military optical Earth observation system currently in operation in Europe. The *Hélios* system is operated by CMOS in collaboration with the CNES Toulouse Station Retention Centre (CMP). Belgium and Spain participate in the program since 2001, Italy since 2005 and Greece since 2007. France's stake remains at 90% (French Senate 2018; Schrogl et al. 2015).

*Pléiades* is the dual-use successor to France's SPOT optical Earth observation satellite constellation and was funded through the Defense Budget Program 191, a dual-use research program (French National Assembly 2016; French Republic 2018a). Access to data from the two *Pléiades* satellites is prioritized to military users. The *Pléiades* satellites are in a sun-synchronous orbit. The first *Pléiades* satellite was launched on 17 December 2011 on a Europeanized Soyuz rocket from Kourou. The second one was launched on 2 December 2012. Austria, Belgium, Spain, and Sweden are participating to the costs of the system in exchange for access to data. The *Pléiades* satellites contribute also to the Optical and Radar Federated Earth Observation system (ORFEO) (Schrogl et al. 2015). *Pléiades* imagery is today commercially available through Airbus GeoStore. *Pléiades* High Resolution (PHR) provides imagery for dual-use with priority for defense users. Imagery to civil users is provided, complementary with *Hélios-2*, via public service delegation to the commercial provider Airbus Defence and Space. *Pléiades* has been

led and run by France in cooperation with Austria, Belgium, Spain, and Sweden. There is also cooperation with Germany via capacity exchange – programming rights – on SAR-Lupe and cooperation with Italy on Synthetic Aperture Radar (SAR) via exchange of data on the dual-use Cosmo-SkyMed (French Senate 2018). In 2019, Airbus and CNES agreed to co-finance a constellation of four Earth observation satellites with a dual purpose for the next 12 years aiming at “providing imagery to the French government, including scientific and military users, and imaging capacity for Airbus to commercialize” (Space News 2019). The first two Airbus-built Pléiades Neo imaging satellites have started comprehensive environmental testing (Airbus 2020).

The *Segment sol d’observation PHAROS* (Portail d’Acces au Renseignement de l’Observation Spatiale) application is a virtual federation of the military Hélios-2, SAR-Lupe, COSMO-SkyMed, and Pléiades systems. PHAROS is enabled through an access portal for imagery intelligence – equally in stationary and deployable configurations – and has been operational since June 2012. PHAROS provides multisensor unified for end users in France and on theatre of operations to all systems, including German and Italian assets. In return of the programming rights negotiated with Italy and Germany on their assets, France has ceded programming rights on Hélios-2 (French Senate 2018).

The *multinational space-based imaging system (MUSIS)* was originally a European surveillance program intended to supply visible, radar and infrared imagery and replace previous national platforms (Bird & Bird 2016). MUSIS today revolves around bilateral cooperation established between France and partnering countries. The *Composante Spatiale Optique (CSO)* is the French space component. France awarded in 2011 a contract to Airbus Defence and Space for CSO-1 and CSO-2 for €795 million. CSO applies to defense users only, with three identical optical satellites. CSO-1 will perform traditional surveillance tasks where CSO-2 will permit target identification. CSO-3 will improve revisiting time. France provides co-funding opportunities to other members of CSO in return for optical imagery. Germany agreed in 2015 to fund 2/3 of CSO-3 for an amount of €210 million. Belgium and Sweden are also cooperating. MUSIS has a similar functionality foreseen as in PHAROS with access to SARah system (Germany), COSMO-SkyMed Second Generation system (Italy), Ingenio system (Spain) and the French legacy components (Hélios). The first CSO high-resolution optical satellite fleet was launched in December 2018, while it is expected to be fully deployed in 2021. The German-French agreement from March 2015 establishing cooperation between radar and optical Earth observation facilitated the implementation of MUSIS (French Senate 2018).

The *OTOS* program (Super-Resolved Optical Earth Observation) is a preparatory program for future generation space satellites for Earth observation and defense running since 2011 – under the name CXCI – until 2020. OTOS is a technological demonstrator that aims to prepare the necessary technologies on the one hand for a future high-resolution post-Pléiades Earth observation program and on the other hand for the rest of the CSO Defence Programme (French Republic 2018a). The *CO3D* program – optical constellation in 3D – is a constellation of optical mini

satellites answering the needs of a of digital terrain model mission and a 3D global model mission for civilian and military needs. These two objectives are based on the same concept of a small satellite with a competitive recurrent cost and a system architecture designed. The launch is foreseen in 2022. The constellation aims to provide continuity for the stereo imagery currently provided by Pléiades (French Republic 2018a).

Regarding big data, the French Ministry of the Armed Forces has defined the requirements for a digital platform to optimize the use of big data capabilities. In April 2018, and following a competitive tender, the French procurement agency DGA selected three companies or groups of companies to take part in the first phase of the *ARTEMIS* (Architecture de Traitement et d'Exploitation Massive de l'Information multi-Sources) innovation partnership. ARTEMIS is a 15-year framework agreement aiming to provide sovereign big data solutions to stay abreast exponential growth in data volumes, transmissions speeds, and formats in the design of information systems (Thales 2018). Six use cases of the project will enable the Ministry of the Armed Forces to take advantage of new capabilities resulting from digital technologies for knowledge sharing, better monitoring of soldiers' health, predictive maintenance of equipment, treatment and visualization of strategic and tactical information (DGA 2019a).

In the context of maritime security, the 2014/2015 project *Trimaran* concerns a concept of a one-stop shop for access, including a range of satellite services for maritime surveillance. In 2016, the French Navy awarded a 4-year contract to a consortium of Telespazio France and Airbus Defence and Space to provide a satellite-based maritime surveillance service. Under *Trimaran 2*, a follow-up to *Trimaran 1*, maritime zone commanders will have access to a portal for surveillance services using optical and radar imaging and AIS (Automatic Identification System) data to enhance the effectiveness of their national maritime missions. The radar and optical satellite images will be interpreted by Telespazio France and Airbus Defence and Space. Reports will then be produced and sent to the users indicating the types of vessels identified and their position, speed, and direction (Airbus 2016).

### **Satellite Communications (SATCOM)**

France's first steps in SATCOM systems were the experimental satellites *Symphonie* and *Telecom 1*. The current French military communications programs are implemented through the French Syracuse program and the French-Italian program *Athena-Fidus* (for the latter see more under the section for *Italy*).

The *Syracuse III System* (Système de Radiocommunication Utilisant un Satellite) is the first exclusive French military satellite communications system, with extremely high frequency (EHF) capacity and a global coverage from Mexico to Indonesia, for at least three theatres of operations simultaneously. Syracuse IIIA military telecommunications satellite was launched in October 2005 and was scheduled to operate for at least 12 years. Syracuse IIIB was launched in 2006. A third satellite, SICRAL 2 was realized in cooperation with Italy and deployed in 2015 with the aim to create redundancy and increase coverage. Syracuse III is maintained to assure transition with Syracuse IV. The SATCOM capability responds to the need

identified in the 2013 White Paper on Security and Defence and assures interoperability with NATO (French Senate 2018). In 2004, the French procurement agency DGA appointed Thales as prime contractor for the Syracuse III ground segment. The contract included the development, acquisition, and through-life support services of the full complement of Syracuse III communication systems and equipment. Thales provided service availability under operational level agreements until 2020 and delivered a total of 600 SATCOM terminals. The contract value amounted to €1.3 billion. Under the Syracuse III program, Thales developed the M21 modem, which successfully completed testing under real jamming conditions in 2003. The modem is compliant with NATO standardization agreement standards. Aristote is one of the central systems in the Syracuse III ground system. Aristote provides communications services between France and units deployed in the theatre of operations and optimizes the transmission capacity of the Syracuse III satellites. The Aristote system's capacity provides the armed forces with the interoperability they require during out-of-area deployments of joint multinational forces on several operational exercises (Defence Aerospace 2004).

*Syracuse IV* was formerly known as COMSAT-NG. In September 2012, the French procurement agency DGA awarded contracts to Thales Alenia Space and Airbus Defence and Space to conduct design studies on the next-generation military satellite communications system as per the military requirements. In December 2015 the consortium agreed to construct and supply the COMSAT-NG telecommunications system. The contract included construction of a ground control segment and Ka-band anchor stations, modernization of ground stations in France, and options for additional satellites. The consortium provided also operations and maintenance support. Thales Alenia Space owns 65% stake in the consortium, while the remaining is owned by Airbus Defence and Space. (French Republic 2018a).

In June 2019, the Ministry of the Armed Forces decided to proceed with the realization of the ground segment of the satellite communications program Syracuse IV. Accordingly, DGA signed a contract with Thales to design and build this capacity. This system brings together space assets (two satellites) and ground assets for users (terminals) and the operator of military networks (land network connection stations, management centers). The Syracuse IVA and Syracuse IVB satellites, ordered at the end of 2015, will be put into service before the end of 2022 to take over from the Syracuse IIIA and IIIB satellites launched in 2005 and 2006. They will be joined by 2030 by a third satellite optimized for use by aeronautical platforms such as increased connectivity, drones, etc. Current ground resources are compatible with these new satellites but must gradually be replaced, modernized, and completed in order to be able to fully exploit the new capacities of these satellites. This will allow the French forces to enhance communications capacities in terms of speed, availability, and resistance to threats, in particular for the equipment that will be delivered during the 2019–2025 Military Programme Law as part of the Scorpion programs; Rafale F4, Defense and Intervention Frigate and Force Supply Building (DGA 2019b).

In support of the Syracuse IV program, Telemak was funded through the *Programme 191 Dual Research*. Telemak activities consist of improving the

performance of Ka-band covers while developing protection against interference and aggression, and to secure ongoing technological developments on the charges useful with a transparent digital processor (French Republic 2018a). Also, FAST is a dual-use project aimed at removing technological risks of the next-generation commercial telecommunication satellites and Syracuse IV, including the development of new generation chips common to civil space and defense programs as well as the development of a positioning, navigation, and timing 3G transparent digital processor (French Republic 2018a).

Overall, the French approach regarding national and multinational SATCOM capabilities development is based on a vision of different layers contributing to the overall capability. The *sovereign core* is composed of Military Satellite Communications Systems (MILSATCOM) with hardened capacity and military use only (Syracuse and SICRAL). The *extended core* is composed of governmental SATCOM with assured access and use by military and public authorities (Athena-Fidus and GOVSATCOM). The *augmented core* complements the picture by adding Commercial Satellite Communications (COMSATCOM) with access upon availability and use by military, public authorities, and civil private customers (EU SATCOM market). France has a long-term position to keep MILSATCOM out of Governmental Satellite Communications (GOVSATCOM) in line with this layered approach. The GOVSATCOM program should give added value to the European Defence Technological and Industrial Base (DGA 2015).

### **Positioning, Navigation, and Timing**

The Ministry of the Armed Forces has access to the civil and military signals of the American Global Positioning System (GPS) system through military receivers developed in France under US license or acquired via Foreign Military Sales (FMS). GPS is evolving, with the introduction of GPS III satellites and the modernization of the ground segment. These changes will require a renewal of the receivers so that they are compatible with the new military signal “Code M,” which will be operational by 2020. OMEGA operation aims to equip the armed forces with jam-resistant receivers and access to several constellations, typically GPS and Galileo (PRS). The realization of the receivers and their integration will be in its majority done after 2019 (French National Assembly 2016).

In the frame of its multiannual program for Research and Technology CNES is looking to prepare the next-generation orbital infrastructures for navigation systems, location, and data collection, improving the performance of technologies, measurement, and systems until 2030/2040, and to prepare, for the short term, technologies and good use of the downstream sector of current generation systems. In 2018, CNES supported time-frequency research aimed at atomic clocks, oscillators and advanced timing and frequency transfer techniques, and performance increase of civil and defense services based on current and future systems, including technologies and relevant signal processing for the user segment. The 2018 call for ideas aimed to meet the future challenges of autonomous vehicles such as drones, transport, agriculture, and miniaturization which requires increase of accuracy, robustness, and integrity of positioning measurements. CNES is preparing for the

evolutions in space infrastructure including GPS system, the deployment of Galileo, multi-constellation mode operations (Galileo, GPS, BEIDOU, GLONASS), as well as the use of satellite-based augmentation system (SBAS) services such as European Geostationary Navigation Overlay Service (EGNOS) and the Wide Area Augmentation System (WAAS) (CNES 2018).

### **Space Situational Awareness (SSA)**

The French dual-use operational Space Situational Awareness (SSA) activities are organized on three levels. At the programmatic and decision-making level, CNES and the French Ministry of the Armed Forces closely cooperate to define policy, capabilities, and priorities. At the sensors level, the Ministry of the Armed Forces operates the *GRAVES* (Grand Réseau Adapté à la Veille Spatiale) survey radar and several tracking radars that CNES uses on a regular basis. CNES together with the National Centre for Scientific Research (CNRS) also operates three TAROT telescopes located at Calern, in Chili, and in La Réunion for survey and tracking purposes. At the operational level, there are two operations centers in France. On the one hand, the military COSMOS Ops Centre of the French Air Force is responsible for Air and Space Defence and reports to the Office of the Prime Minister, as provided for by the French Code of Defence. On the other hand, the CNES Ops Centre consists of a 24/7 on-call team of ten specialists dedicated to conjunction assessment, alerts, and recommendations of collision avoidance maneuvers to spacecraft operators and owners (UNCOPUOS 2017).

After approaches and inspections of French satellites by foreign governments, Air Force Gen. Jean- Pascal Breton of the French Joint Space Command stated in January 2018 that the capability to detect and identify the suspect of an unfriendly or aggressive act is an “essential condition for protection.” The capability to track exo-atmospheric space activity will be gradually “strengthened to allow identification and classification of objects in orbits that are of interest to France,” he added. France first introduced a space surveillance asset called *Stradivarius* located in Celar, in Brittany. France was obliged to dismantle its space surveillance asset recognizing the “space-dominant” role of the USA in NATO (Defence News 2018b).

The current *GRAVES* system is operated by the French Air Force. It is the space component of France’s *SCCOA* (*Système de Commandement et de Conduite des Opérations Aérospatiales*, System for Command and Control of aerospace operations) (French National Assembly 2016). *GRAVES* was developed by ONERA (*Office National d’Etudes et de Recherches Aérospatiale*, French national aerospace research center), which was delegated by DGA. It took 15 years for the installation to become operational in November to December 2005. *GRAVES* is composed of a bi-static radar installation – emission site near Dijon and reception site near Albion – and exploitation server located at the Air Force base of Lyon Mont Verdun. Operations are performed by COSMOS (*Centre Opérationnel de Surveillance Militaire des Objets Spatiaux*) (ONERA 2016).

The *GRAVES* functionality ranges from modelling the passage of foreign observation or listening satellites to the detection of new objects such as spy satellites. *GRAVES* had detected the orbital presence of “anomalies,” in other words satellite



browser spies, especially US ones. Expanded surveillance French space allowed by GRAVES led to a strategic deal with the US, with both partners keeping the information on each military asset in space classified. Information on France's military satellites is therefore no longer available on open US sources. At the national level, the strategic benefit of the investment represented by GRAVES in terms of spatial surveillance is perceived as very high, even more considering the relatively minor cost of the system at €30 million. In this regard, GRAVES aims to strengthen the status of France as a strategic partner of the US (French National Assembly 2016).

To continue to give France leverage in terms of influence and to keep a central place in the future European Space Surveillance and Tracking (SST) architecture, improvements to GRAVES are required in addition to sharing the capabilities with partners. A 2012 report submitted to the French Senate identified the following actions to be taken: GRAVES obsolescence treatment activities, installation of additional sensors, and inching identification capabilities through optical imagery. Identification is currently achieved through the assistance of the German Tracking and Imaging Radar (TIRA). France and Germany have concluded an agreement for sharing GRAVES and TIRA data. France is considering how it can achieve this capability at national level without dependency on partner assets and capabilities (French National Assembly 2016). At the end of 2016, a maintenance in operational condition – renovation – contract was concluded between DGA and ONERA/Degreane Horizon (Groupe Vinci Energies) for the maintenance activities allowing the GRAVES infrastructure to remain operational until 2030 for €40 million. The contract was awarded for 5 years with a further option for 3 years of operations. Apart from that initial modernization, ONERA is studying options for future upgrades which would allow the system to detect mini satellites weighing less than 500 kg and micro-satellites weighing less than 150 kg (ONERA 2016). The European Union Space Surveillance and Tracking (SST) Support Framework contributes to these activities. In the current condition, GRAVES does not detect all sizes of satellites. The ongoing renovations will enhance capabilities, but detection of nanosatellites is expected to be achieved only by 2025 (ONERA 2016).

Commissioned in 1992, *Monge A601* is a missile-range instrumentation vessel, flagship of the Trials Squadron, and belongs to the DGA. The vessel has DRBV 15C air search and two navigation radars; its mission equipment includes the Stratus Gascogne, Armor (two), Savoie and Antares (two) missile tracking radars, a laser radar, an optronic tracking unit, and 14 telemetry antennae (FRS 2015). Monge could be partially used for SST functions like acquisition of orbital parameters in LEO. Monge can monitor missile launches including the Ariane rocket family. The Monge SATCOM system was made compatible with Syracuse III in 2015 after a major refit (FRS 2015).

*SATAM* is composed of four radars belonging to the French Air Force and is used for air defense purposes. *SATAM* may perform additional tracking in low Earth orbit. The tasks are implemented by the Air Force Command based on requests by COSMOS (FRS 2015). The radars are used for monitoring debris for management of

collision risk determination and atmospheric reentry analysis. OSCEGEANE (Observation Spectrale et Caractérisation des Satellites Geostationnaire) is an experimental project to determine spectral signature of GEO objects. Operations are undertaken by COSMOS (French Joint Space Command 2016).

The LPM 2019–2025 foresees a modernization of GRAVES and SATAM, also using the opportunities presented by a future EU SST/SSA program (French Republic 2018b).

### **Electronic Intelligence (ELINT)**

Since 1995 France has been placing experimental ELINT payloads and satellites in orbit. The objective is to eventually have satellites that allow France to figure out the location of and, where possible, identify individual transmitters and radars. This information would help French forces avoid detection in any military conflict, but initially the objective has been to understand how much information can be obtained to justify the funding of a future operational system (Schrogl et al. 2015).

France operates *ELISA*, an experimental electronic intelligence satellite, due to be replaced with the operational CERES system in 2020. ELISA (Electronic Intelligence Satellites) is a demonstration project, composed of four small satellites that were launched in December 2011, for spotting radar and other transmitter positions. The project is run and operated by DGA and CNES, who tasked EADS Astrium as a prime contractor with developing the space segment. ELISA could lead to an operational program of space-based electronic intelligence. Like Essaim, the ELISA satellites used the Myriade platform with a mass of roughly 130 kg each (Schrogl et al. 2015). Essaim (French for “swarm”) was a family of four small satellites for electronic intelligence. They were commissioned by DGA, and they were launched on 18 December 2004 (together with, among others, Helios-2A) from Kourou. The Essaim constellation deorbited in 2010 (Schrogl et al. 2015).

The *CERES* (Capacité de Renseignement Électromagnétique Spatiale) military electronic intelligence mission will use three formation-flying satellites detecting and locating radio communications and radars (Bird & Bird 2016). Preparatory phases of the project started in June 2007. DGA signed a contract with Airbus Defence and Space in December 2015 for the three satellites in low Earth orbit with an estimated program cost of €400 million. The objective of CERES is to provide the ability to intercept and locate electromagnetic emissions – radio communication and radar – from space. The CERES system forms part of the national joint force intelligence chain by contributing to permanent monitoring, surveillance, and support for operations. The CERES program aims at obtaining an operational listening capacity allowing the interception and localization of electromagnetic emissions from space (French Senate 2018). CERES will be using ISIS. The ISIS project (initiative for space innovative standards) is the production of an interoperability repository based on a line of ground segment products for generic control of next-generation satellites (French Republic 2018a).

According to the LPM 2019–2025, early warning contributes to surveillance of proliferation and ballistic activity; the identification of potential aggressors, with a

view to the implementation of deterrence or conventional counterforce actions; alert populations based on the estimated areas targeted; and meet NATO commitments. NATO planned in November 2010 to establish a full anti-missile defense capability, the NATO Integrated Air and Missile Defence System. France aims to contribute to this system by 2020–2021. System architecture studies conducted in 2011–2012 confirmed the interest in developing two types of complementary sensors: space-based optical sensors with infrared detectors and very long-range UHF radars installed on land or at sea (French Senate 2018).

The first ability was tested by the SPIRALE program. *SPIRALE* was a French space-borne early warning capacity demonstrator (*Systeme Preparatoire Infra-Rouge pour l'Alerte*) consisting of two satellites launched in 2009 and remaining in orbit until 2011 (French Ministry of the Armed Forces 2012). Between 2002 and 2011, for a total cost €137 million, an Earth database essential to understanding natural and physical phenomena likely to generate false alarms was created. For budgetary reasons, the continuation of the program has been postponed beyond military programming for 2014–2019.

Regarding the radar component of the system, a demonstrator of a very long-range radar was ordered in 2011 and completed in 2016. The radar is currently in testing and validation phase. The originally envisaged timetable, which provided for a delivery of an early warning system in 2021, was considered unrealistic given the resources provided for in the LPM 2014–2019. However, the 2017 Strategic Defence Review and National Security Council expressly confirm the interest of the project. The acquisition of an early warning system is open to cooperation. In this respect, it should be noted that France, Italy, and Turkey signed a letter of intent in November 2017 to strengthen their cooperation in the field of armaments, including missile defense (French Senate 2018).

In the frame of NATO, France contributes to the ALTBMD Program (Active Layered Theatre Ballistic Missile Defence). Missile launch detection, tracking, and warning activities are implemented through cooperation with the US and the Space-Based Infrared System (SBIRS). Regarding anti-missile capabilities, France has a ground-air system called SAMP/T, the ballistic anti-missile capability of which has been demonstrated in 2011. In addition to the 10 ground-based road mobile SAMP/T batteries, France holds the Principal Anti Air Missile System (PAAMS), the S1850M Radar, and the European Multifunction Phased Array Radar (EMPAR), all implemented on two Horizon-class frigates, and 12 ground-based road mobile Crotale Next Generation short-range air defense batteries (French Ministry of the Armed Forces 2012).

Fibally, ONERA is conducting a technology demonstrator, dubbed DRTLTP, for an over-the-horizon radar to detect and track ballistic missile launches. ONERA took delivery in 2017 of the demonstrator built on a reduced scale of one-eighth for a very long-range radar, and tests have begun in 2018. The demonstrator studies a capability to detect and track a missile launch and forecast the point of impact and studies detection and tracking of satellites. ONERA aims to optimize the technology with upstream research allowing the DGA to decide how to pursue the project. (Defence News 2018c).

## Germany

### Space and Security Budget

Germany's estimated defense expenditure was €42.12 billion or 1.38% of GDP in 2018, below the NATO guideline of 2% of GDP. 16.6% of the 2018 estimated budget was allocated to equipment expenditure. To reach NATO's 2% of GDP target by 2024, defense expenditures would have to more than double within 7 years (NATO 2019). German government space expenditure was estimated at €1.9 billion in 2018 including €1.74 billion for civil activities and €166 million for defense (Euroconsult 2019). The 2018 budget increased by 1% compared to 2017. The breakdown of civil space expenditures between the national and ESA programs has remained constant since the beginning of the decade, with national programs receiving between 43% and 45% of the budget and the rest going to ESA. In 2018, Germany was the second largest contributor to ESA, almost on par with France. The German contribution grew 7% in 2018, reaching €920million. Defense space expenditure is not publicly released (Euroconsult 2019).

### Space and Security Activities and Programs

#### Earth Observation (EO): Intelligence Surveillance-Reconnaissance (ISR)

In November 2017, OHB System AG was awarded a contract for the development of a global electro-optical satellite system, nicknamed "Georg. This was intended for reconnaissance and consisted of two satellites to be placed under the authority of the German Secret Service (BND). The rationale for the system was to guarantee assured access and direct access to electro-optical imagery for German intelligence. The contract amounted to €400 million and the satellite is expected to be launched in 2022 with full operational capacity in 2022–2023 (La Tribune 2017). The budget was approved in June 2017. When the German government signed the contract with OHB, some French observers criticised Berlin of walking back on Franco-German agreements – with France focusing on electro-optical sensors and Germany on radar and partners exchanging data – adding that Germany had yielded to influence from its national space industry and refusing French industrial expertise (International Institute for Strategic Studies 2017).

SAR-Lupe is Germany's first satellite-based reconnaissance system. SAR-Lupe is a SAR (Synthetic Aperture Radar) reconnaissance satellite imaging project of the German government, implemented by the German Ministry of Defense (BMVg) and the former Federal Office of Defence Technology and Procurement (BWB). The SAR-Lupe program consists of five identical (770 kg) satellites, launched between December 2006 and July 2008 and developed by OHB System AG as prime contractor. The satellites are controlled by a ground station operated by the Bundeswehr Geoinformation Centre (BGIC) under the Strategic Reconnaissance Command (KSA). Within the KSA, the Zentrale Abbildende Aufklärung (ZentrAbbAufkl) operates the user segment for SAR-Lupe. Delivery of the overall

system was officially accepted by the Federal Office of Equipment, Information Technology and Utilization (BAAINBw), in September 2008. A bilateral agreement (Schwerin Agreement) with the French government was signed in 2002 for data from SAR-Lupe to be provided in exchange for data from Helios ([OHB Website](#)). The SAR-Lupe original program cost was €350 million (Satellite Observation 2016). Operating in X-band, the radar satellites have two modes. The first mode “stripmap,” in which the satellite maintains a fixed orientation regarding Earth, provides extended time imaging with a fixed direction of the antenna. The second one “spotlight,” in which the satellite or the sensor direction rotates to keep pointing at a specific target area, is used for high-resolution imagery. The actual resolution values of SAR-Lupe are classified. The only official statement is that the spatial resolution is much better than 1 m (Schrogl et al. 2015). Germany’s development of this program was directly related to its experiences during the NATO action in Kosovo, particularly to difficulties in getting the US to share satellite intelligence of direct relevance to the protection and security of non-US allied forces. These experiences convinced Germany of the need for its own space-based intelligence-gathering assets (European Parliament 2006).

In July 2013, OHB System AG signed a contract with the Federal Office of Equipment, Information Technology and Utilization (BAAINBw), within the German Armed Forces, to develop the *SARah* (Satellite-based Radar Reconnaissance) system consisting of three second-generation satellites aimed to replace the SAR-Lupe constellation. OHB agreed to build two passive-antenna Synthetic Aperture Radar (SAR) satellites at 500 km non-SSO orbits, and Astrium GmbH would build a larger, phased-array-antenna satellite at 750 km SSO dawn-dusk orbit under contract for OHB (SpaceX 2013). In 2019 BAAINBw signed an additional contract with OHB adjusting the initial requirements to implement the *SARah* system in response to threats in the area of IT security and satellite communications (Bloomberg 2019). The system with one ground station is planned to be delivered and to become operational in 2020 after launch on SpaceX Falcon 9. The ground segment for *SARah* is already operating the SAR-Lupe satellites as of February 2018. Germany is in the process of preparing the *SARah* next-generation system with decisions to be taken before the end of 2020 to ensure seamless transition between systems ([EO Portal Website](#)).

Germany had considered in the past establishing *HIROS* (High-Resolution Optical System) in close collaboration with the US. *HIROS* was to be a triplet optical satellite expected to be built by OHB System AG. After funding issues at the German Secret Service (BND) side, efforts were dropped (Satellite Observation 2016). The German Ministry of Defense, instead, decided to invest €210 million in the French CSO system (*Composante Spatiale Optique*) in 2015, the follow-up project of Helios-2 (La Tribune 2017).

*TerraSAR-X/TanDEM-X* is a high-resolution interferometric SAR (Synthetic Aperture Radar) mission of the German Aerospace Center, DLR, together with the partners EADS Astrium GmbH and Infoterra GmbH in a Public Private Partnership consortium (Schrogl et al. 2015). The mission concept is based on a second *TerraSAR-X* radar satellite flying in close formation to achieve the desired

interferometric baselines in a highly reconfigurable constellation (Schrogl et al. 2015). The elevation model yields important information to military planners preparing for tasks such as special forces operations, target designation for bombings, and surveillance missions. Following an announcement from DLR in October 2016, the TanDEM-X global elevation model was completed, exceeding the 10-meter accuracy. Between January 2010 and December 2015, the two radar satellites transmitted more than 500 terabytes of data to Earth via the worldwide reception network. In parallel, systematic creation of elevation models began in 2014. TerraSAR-X and TanDEM-X have long exceeded their specified service lives and continue operating (DLR 2016). Airbus Defence and Space holds the commercial marketing rights for TanDEM-X data, worth €359 million for the data licenses, processing software, and running costs. The US had urged Germany to grant access to the TanDEM-X global elevation model (Spiegel 2015). Airbus Defence and Space and the German Ministry of Defense subsequently signed a contract for the utilization of TanDEM-X mission data. On 14 December 2015, the US National Geospatial-Intelligence Agency and the German Bundeswehr Geoinformation Centre signed an agreement to strengthen worldwide geospatial data-sharing partnerships and increase the accuracy and quality of NGA products and services (NGA 2015).

Building on the success of TanDEM-X, *Tandem-L* is a DLR proposal for a highly innovative radar satellite mission to monitor dynamic processes on the Earth's surface with hitherto unknown quality and resolution. Important mission goals include the global measurement of forest biomass, the systematic monitoring of deformations of the Earth's surface, the quantification of glacier motion and melting processes in the polar regions, and observations of the dynamics of ocean surfaces and ice drift. The implementation of Tandem-L means a worldwide unique remote sensing system exceeding the performance of existing systems. According to current planning, the Tandem-L satellites could be launched in 2023 (DLR Tandem-L). In addition, the *TerraSAR-X NG* is intended to succeed the current TanDEM-X and TerraSAR-X. The TerraSAR-X NG mission is intended to take the data and service continuity well beyond 2025 taking benefit of a 9.5 years satellite lifetime. The space segment, initially a single spacecraft, will be launched into the reference orbit, while the first-generation systems will still be operational. This is a project of Airbus Defence and Space Geo-Intelligence/Infoterra GmbH, Friedrichshafen, Germany (EO Portal Website).

*EnMAP* (Environmental Mapping and Analysis Program) is a hyperspectral satellite mission that aims at monitoring and characterizing the Earth's environment on a global scale. EnMAP serves to measure and model key dynamic processes of the Earth's ecosystems by extracting geochemical, biochemical, and biophysical parameters, which provide information on the status and evolution of various terrestrial and aquatic ecosystems. The EnMAP long-term program is based on a cooperative approach involving various German institutions including DLR and the German Research Center for Geosciences. In November 2006, DLR awarded a design contract to Kayser-Threde GmbH (OHB owned) as prime contractor of EnMAP. In 2008, a contract for the realization phase was signed for a total contract value of €90 million. Launch is expected for 2021 (OHB 2008).

The *RapidEye* mission was a commercial remote sensing mission by the German Company RapidEye AG. It was supported by German Aerospace Center (DLR) with funds from the Ministry of Economics and the Brandenburg state government. The total sum invested in the project amounted to around €160 million, of which about 10% is funded by DLR. The RapidEye's complete constellation of five satellites was successfully launched on a single DNEPR-1 rocket (a refurbished ICBM missile) on 29 August 2008 from the Baikonur Cosmodrome in Kazakhstan and became commercially operational in February 2009. In November 2013 RapidEye officially changed its name to BlackBridge (Schrogl et al. 2015). The RapidEye constellation was acquired by Planet Labs, a US private company, in 2015.

The DLR *FireBIRD* (Fire Bispectral InfraRed Detector) mission consists of a pair of satellites – TET-1 (Technology Experiment Carrier) and BIROS (Bispectral Infrared Optical System) – that detect high-temperature events from space. Both satellites are based on the small satellite BIRD – operational from 2001 to 2004 – which was developed by the DLR Institute of Optical Sensor Systems. TET-1 has been orbiting Earth since 2012. BIROS has also been in orbit since 2016, adopting an open constellation to support TET-1. The satellite data is mainly received at the DLR ground station in Neustrelitz and then processed, archived, and made available worldwide for scientific purposes by the German Remote Sensing Data Center. FireBIRD has the capability to detect smaller fires. This enables more precise mapping and therefore analysis of their impact on the climate (DLR 2017a).

The German Remote Sensing Data Center (DFD) is an institute of DLR. DFD and DLR's Remote Sensing Technology Institute (IMF) together comprise the Earth Observation Centre (EOC). With its national and international receiving stations, DFD offers direct access to data from Earth observation missions, derives information products from the raw data, disseminates these products to users, and safeguards all data in the National Remote Sensing Data Library for long-term use. The DFD Ground Station Network consists of stations located in Germany, Canada, and Antarctica (DLR 2018). DLR signed a bilateral cooperation agreement with the Canada Centre for Remote Sensing (CCRS) for receiving satellite data in Canada. The CCRS makes land available in the context of this contract. The commercial partner, PrioraNet Canada (PNC) – a joint venture between the Canadian company Iunctus Geomatics and the Swedish Space Corporation – has been responsible for the maintenance and development of the site. The Antarctica station has been important in the frame of data reception for the TanDEM-X mission (DLR 2018).

The Fraunhofer Institute is developing a *nanosatellite ERNST* (experimental spacecraft based on nanosatellite technology) to reduce development costs and time to orbit. When carried into orbit in 2021, ERNST will be equipped with an infrared camera for Earth observation. ERNST will be put in a 700 km SSO orbit. The main purpose of the ERNST is to evaluate the utility of a 12 U nanosatellite mission for scientific and military purposes (Fraunhofer 2018).

In the field of *HAPS* (high-altitude platform station), a start-up company called Alphalink, in cooperation with the Technical University of Berlin, is developing a high-altitude platform for delivering Internet connection to remote locations. Interest in the applications has been shown by disaster management institutions, the Federal

Office of Disaster Management and Civil Protection in Germany, as well as the International Disaster Management Association (Space News [2017a](#)).

### **Satellite Communications (SATCOM)**

Germany currently holds two communication satellites, COMSAT 1 and COMSAT 2, and ground stations (*SATCOMB<sub>w</sub>* system). *SATCOMB<sub>w</sub>* system is the first owned, dedicated communications system of the German Armed Forces. DLR's German Space Operations Centre (GSOC) is responsible for monitoring and controlling the spacecraft. The satellites were launched in October 2009 and May 2010 to geostationary orbit with an orbital lifetime foreseen of 15 years ([Air Force Website](#)). The German Armed Forces awarded a contract to a team led by MilSat Services in July 2006, to carry out *SATCOMB<sub>w</sub>* stage 2 military communications program for 10 years. The contractual scope included in-orbit delivery and operation of two communications satellites, development of anchor station and ground user terminal segment, as well as modernization of the central command, control, and network management centers. Germany had also awarded a subcontract to Thales Alenia Space to design, build, integrate, test, and deliver COMSATBw-1 and COMSATBw-2 satellites. Tesat, a subsidiary of Airbus Defence and Space, supplied the payloads ([Air Force Website](#)).

In March 2016, Airbus Defence and Space GmbH was awarded a contract from the German Armed Forces procurement agency – BAAINBw for continued operations of the *SATCOMB<sub>w</sub>* satellite communications system until 2022 ([Shephard 2016](#)). Germany is currently defining requirements for the future systems replacing the existing *SATCOMB<sub>w</sub>* stage 2 capacities. COMSAT 1 and COMSAT 2 will reach their end of life by 2027. To fill this potential gap, prospective solutions are investigated including acquisition and in-service aspects also in the frame of future EU and NATO programs ([IAI 2018](#)).

DLR signed in July 2017 a contract with OHB Systems for an experimental telecommunications satellite, *Heinrich Hertz*, that will be used partly by the Federal Armed Forces. The launch of the satellite is expected in 2021. The mission aims to explore and test new communications technologies in space at a technical and scientific level. *Heinrich Hertz* will carry approximately 20 technology experiments as well as a fully functioning Ku- and Ka-band military communications payload. *Heinrich Hertz* will use the SmallGEO satellite platform designed under the European Space Agency's ARTES program. DLR is responsible for *Heinrich Hertz*'s project planning and implementation, while the Ministry for Economic Affairs and Energy is financing the program ([OHB Website](#)).

Furthermore, within the project OSIRIS, optical communication systems are optimized especially for small satellites that are developed. To enable robust communication links, DLR also deals with the development and implementation of forward error correction algorithms which are optimized for free-space optical communication links ([DLR 2017b](#)).

Germany has developed a satellite-based Modular Warning System (MoWaS), for defense and crisis situations, and has also made it available to the federal states as a central warning and information system ([BBK 2017](#)). In order to cope with crises, the



federally owned satellite-supported warning system (SatWaS) was developed since 2001. The further development of SatWaS into the Modular Warning System (MoWaS) was completed in 2013. This is geographic information system (GIS)-based. Through a single transmission protocol, MoWaS can control all the devices and applications imaginable today (such as smoke detectors, mobile devices, apps). This includes already existing but also future warning channels. This is possible by using the Common Alerting Protocol as the open data format of the alerts (BBK 2017).

### **Positioning, Navigation, and Timing (PNT)**

In September 2017, the German Ministry of Defense selected Rockwell Collins' NavHub navigation system to provide GNSS availability to a variety of its military vehicles. The NavHub system serves as a next-generation GNSS- and military-code (M-code)-enabled solution for the German Armed Forces. Customizable for ground and maritime platforms, NavHub provides a variety of vehicle interfaces, meets the standards required by military vehicle operators, and allows users to receive data from multiple secure and open-service GNSS constellations to simultaneously confirm the navigational solution (Selective Availability/Anti-spoofing Module (SAASM) GPS receivers). Access to multi-constellation GNSS and GPS M-code provides a significantly enhanced navigational solution over the GPS-only solution (GPS World 2017). Since 2014, the German government has been sponsoring a special prize for Public Regulated Service (PRS) applications as part of the European Satellite Navigation Competition (ESNC), with the aim to perform joint testing activity with Belgium and other Member States and advance technology on further miniaturization and simplification of PRS receiver technology (GSA 2017).

The Institute of Communications and Navigation of DLR is involved in development of many advanced signal processing algorithms for GNSS applications with stringent requirements toward service performance and reliability. DLR's Multi-output Advanced Signal Test Environment for Receivers (MASTER) is a unique and powerful hardware simulation tool for testing and quality assessment of Global Navigation Satellite System (GNSS) Receivers (DLR Website). In addition, the *German Satellite Positioning Service* (SAPOS) has set up and permanently operated a multifunctional differential GNSS service. The system is based on a network of approximately 270 GNSS reference stations which are operated by the Surveying Authorities of the States of the Federal Republic of Germany (AdV). This service is widely available with high reliability and comprises three service areas with different properties and accuracies (AdV Website).

### **Space Situational Awareness (SSA)**

The Space Situational Awareness Centre (GSSAC), run jointly by the German air Force and DLR, operates the *Tracking and Imaging Radar* (TIRA) system, which is owned by the Fraunhofer Institute (French National Assembly 2016). TIRA is an adapted radar to track objects in low Earth orbit through

characterization and localization. TIRA performs the “characterization and track” phase but needs input from other kinds of radar, like the French GRAVES, to survey the space zone and identify the object that needs to be observed and tracked (FRS 2015). France and Germany have an agreement for sharing GRAVES and TIRA data (French National Assembly 2016). TIRA’s typical tasks, apart from orbit determination and damage analysis, include the identification and technical analysis of satellites. This is possible due to its radar images which are characterized by high radiometric and spatial resolution. All phases of the space mission, extending from the launch and operational phases to the reentry phase, can be supported with the radar data from TIRA. TIRA has monitored the reentry of the Chinese Space Station Tiangong-1 in 2018 (Fraunhofer Institute 2018).

In 2016, Germany decided to expend its SSA center originally established in 2009, in the aftermath of the 2007 Chinese Fengyun-1C ASAT test. The Centre is run jointly by DLR and the German Air Force. The new German Experimental Space Surveillance and Tracking Radar, or GESTRA, became operational in 2019. The new space surveillance radar GESTRA (German Experimental Space Surveillance and Tracking Radar), which is currently being developed by Fraunhofer Institute for DLR, is equipped with an electronically steerable antenna that can scan large areas of the sky based on semiconductor technology. GESTRA is designed to operate continuously to create a catalogue of the debris in near-Earth space (Fraunhofer Institute 2018). GESTRA received its first signals reflected by objects in space on 27 November 2019 (DLR 2019).

---

## Italy

### Space and Security Budget

Italy’s defense expenditure was €21.18 billion or 1.22% of GDP in 2018, below the NATO guideline of 2% of GDP (NATO 2019). The Italian government expenditure for space-related activities amounted to €1 billion in 2018 of which €950 million covered civil activities and €50 million defense (Euroconsult 2019). ESA represented 61% of Italy’s civil space budget in 2018 at €578 million. Earth observation is the largest area of investment of the Italian space program representing 43% of the national civil expenditures in 2018, which is 24% of the civil budget. The budget for defense space programs is based on the procurement cycles of the national Earth observation and satellite communications systems. The defense space budget reached its lowest level across the decade at €50 million in 2018, following the launches of Athena-Fidus (2014), SICRAL 2/Syracuse IIC (2015) and the optical satellite SHALOM (2017) (Euroconsult 2019).

## Space and Security Activities and Programs

### **Earth Observation (EO): Intelligence Surveillance-Reconnaissance (ISR)**

*COSMO-SkyMed* is the first space-borne Earth observation system implementing a dual-use architecture for civilian and defense needs in both national and international contexts. The system has been commissioned and funded by the Italian Space Agency (ASI) and the Italian Ministry of Defence in 2003 with Thales Alenia Space Italy (TASI) as prime contractor. The system design and development has been led by TASI in collaboration with a large industrial team comprising many other small- and medium-sized Italian companies mainly belonging to the Finmeccanica Group. The dual nature of the system can be retrieved already in its mission objectives relating mainly on the capability to provide information and services useful for many activities and applications for both civilian and defense users (Schrogl et al. 2015).

The COSMO-SkyMed system consists of a space segment composed by a constellation of four low Earth orbit mid-sized very high-resolution satellites, each carrying a multi-mode high-resolution Synthetic Aperture Radar (SAR) instrument. Both ground and space segments are conceived to support dual-use, the space segment thanks to an antenna granting a wide spread of resolutions and swaths, whereas the ground segment thanks to the duplication of its key elements and a series of rules and procedures granting a secure data circulation. The success achieved by this space-borne mission is testified by the interest that it has generated in other countries. As such, ASI operates as a procurement agency for the French defense administration. The COSMO-SkyMed French defense user ground segment is fully operative, and according to Italian and French government partnerships, a bilateral image-trading protocol has been established: COSMO-SkyMed SAR image products are exchanged with Helios-2 optical image products to support institutional defense applications (Schrogl et al. 2015). Thales Alenia Space and Arianespace signed in September 2017 a launch contract for two COSMO-SkyMed Second Generation (CSG) satellites manufactured for ASI and the Italian Ministry of Defence (Arianespace 2017a). The CSG COSMO-SkyMed constellation is a satellite system designed to ensure operational continuity of SAR observation services provided by the four first-generation COSMO-SkyMed satellites, launched between 2007 and 2010 (Telespazio 2019). Built by Thales Alenia Space, the CSG COSMO-SkyMed satellites will each weigh approximately 2.3 tons at launch and will be positioned in SSO dawn-dusk orbit at an altitude of 619 km (Defense Aerospace 2017). The first CSG COSMO-SkyMed (CSG-1) was launched from the Kourou European Space Centre in French Guyana on December 18, 2019.

In June 2017, OHB Italia and Arianespace announced the signature of a Vega launch contract in 2018 for *PRISMA* (*Precursore iperspettrale della missione applicative*). PRISMA is an Earth observation satellite fitted with an innovative electro-optical instrument, combining a hyperspectral sensor with a medium-resolution panchromatic camera (Arianespace 2017b). The PRISMA mission main objectives are the in-orbit demonstration and qualification of an Italian state-of-the-art hyperspectral imager, the implementation of a preoperative mission and the

validation of the end-to-end data-processing chain for new applications based on high spectral resolution images. This allows to provide products for environmental observation and support to risk management. The PRISMA Space Segment consists of a single satellite placed on a Sun-synchronous low Earth orbit and an expected operational lifetime of 5 years. PRISMA is civilian system under civil control, but the Italian Ministry of Defence has demonstrated interest in its applications including agriculture, environment, climate change, and costal monitoring (Loizzo 2016).

*OPTSAT-3000* consists of a satellite in a Sun-synchronous low Earth orbit and of a ground segment for in-orbit control and for data acquisition and processing. OPTSAT-3000 aims to provide high-resolution images of any part of the globe, providing Italy with an autonomous national capability of Earth observation from space with a high-resolution optical sensor. The system is supplied by Leonardo through its joint venture Telespazio. As prime contractor, Telespazio leads an international group of companies including, among others, Israel Aerospace Industries, which built the satellite within an international cooperation agreement between Italy and Israel as well as OHB Italia that is responsible for the launch and will make use of the VEGA European launcher. OPTSAT-3000 will jointly operate with the second-generation COSMO-SkyMed system of radar satellites – which has also been developed by Italian industry. Thales Alenia Space and Telespazio integrate optical and radar data to provide the Italian Ministry of Defence with accurate information and state-of-the-art analysis (Leonardo 2017). OPTSAT was launched with Vega from Kourou on 2 August 2017. The OPTSAT-3000 program was developed to provide an independent, national high-resolution optical space-based Earth observation capability, integrated with the first- and future second-generation COSMO-SkyMed SAR satellite constellation in support of the requirements of the Italian Ministry of Defence, as well as national agencies operating in the field of safety and security and international customers (Janes.com 2017).

The *SHALOM* (*Spaceborne Hyperspectral Applicative Land and Ocean Mission*), which is in collaboration with the Israel Space Agency (ISA), may be considered as an upgraded OPTSAT-3000 satellite regarding hyperspectral imagery). SHALOM and OPTSAT-3000 give Italy key space intelligence capability, based on defense cooperation between Italy and Israel (Janes.com 2017). The mission objectives are to provide high-resolution (spectral, spatial, temporal) data of geochemical, geo-physical, and geo-biological variables; provide thematic digital maps of the above parameters such as environmental quality, crisis monitoring, search for mineral and natural resources, monitoring water bodies, and assisting precision agriculture activity; enable quantitative measurement of currently immeasurable (space) parameters that are required by a wide range of end users; and provide high-quality calibrated data as input for generating thematic maps and models for monitoring those parameters (Janes.com 2017). ASI and Israel Space Agency signed in 2015 an agreement for the development of the SHALOM mission (EARSC 2015).

### **Satellite Communications (SATCOM)**

*SICRAL* (*Sistema Italiano per Comunicazioni Riservate e Allarmi*) is Italy's first dedicated military telecommunications satellite and was the product of the industrial

consortium comprising Alenia Spazio (70%), FiatAvio (20%), and Telespazio (10%) (European Parliament 2006). The program is divided into three phases. The first began in 2001 with the launch of the SICRAL 1, a satellite that is still in operation. The second phase began in 2009 with the launch of SICRAL 1B, which has an estimated operational life span of 13 years (Telespazio 2020a). The third phase, in cooperation with France (see above in the section of France), became operational after April 2015 with the launch of SICRAL 2, with an estimated operational life span of 15 years. SICRAL 2 is a geostationary satellite, able to enhance the capability of military satellite communications already offered by SICRAL 1 and SICRAL 1B and by France's Syracuse System. SICRAL 2 supports satellite communications for the Italian and French Armed Forces, anticipating the needs of growth and development in the next few years. The satellite has an additional backup function to the current capacity of the French Syracuse III system and that of SICRAL 1B allocated to NATO communications (Telespazio 2020b).

### **Positioning, Navigation, and Timing (PNT)**

The Italian Space Agency (ASI) Strategic Document 2016–2025 has a dedicated section on Galileo including a Galileo Public Regulated Service (PRS) national program, considered an area of strategic importance. For Italy, the real challenge and opportunity for the future come from the integration of downstream services of navigation with services of telecommunications and Earth observation. To take advantage of these opportunities, a national support program, the Mirror Galileo, is being studied and envisages the development of MEO (Medium Earth Orbit) platforms for navigation payloads, to facilitate the competitiveness of our national industry in the upstream sector, technological developments for Galileo components and subsystems, and also in a developmental perspective (ASI 2016).

The *PRESAGO* project, with the involvement of potential institutional domestic users, has defined the preliminary design of the baseline PRS, that is of the infrastructures, systems, and services necessary for supporting and making the use of the PRS efficient, both inside and outside of the national borders. The domestic program for the Galileo PRS infrastructure comprises national capability for manufacturing PRS receivers, including relative security modules, and the development of domestic activities. The latter consist of the development of the PRS security center, the interference monitoring system, the PRS terminals, the network and interfaces for domestic users, etc. The main benefits expected are the possibility for Italy to use its own infrastructure to support other European countries in using the PRS services; the access to the potential market relative to the implementation of PRS structures by other European countries; the development of value-added service solutions, based on the concept of PRS servers; and the development of value-added service solutions that integrate other satellite technology solutions (ASI 2016).

A private network of more than 150 Global Navigation Satellite Systems (GNSS) permanent sites, named ItalPoS (Italian Positioning Service) and uniformly covering the entire Italian territory, was established in April 2006 by the Italian Division of Leica Geosystems S.p.A. This network also involves several GPS stations of the INGV (Italian National Institute of Geophysics and Volcanology) RING (real-time

Integrated National GPS) network and GPS stations from other public and private bodies (Castagnetti et al. 2010).

### **Space Situational Awareness (SSA)**

The ASI Strategic Vision document outlines the Italian plans for contributing to EU SST. ASI is expected to make available the sensors located at the SGC (Space Geodesy Centre). The role of SGC is that of Centre of Expertise for Civil Protection in monitoring the uncontrolled reentry of space debris. The Ministry of Defence will contribute, with optical telescopes and radar used for detection and tracking, together with the National Operations Centre. INAF (the National Institute for Astrophysics) will contribute with the Sardinia Radio Telescope and the “Northern Cross” Radio Telescope located in Bologna (ASI 2016).

The Matera Laser Ranging Observatory (MLRO) is owned by ASI and operated by e-GEOS. The observatory provides very precise laser ranging for satellites, suitable for satellite tracking applications. The observatory has not yet been tested for space debris tracking. The SPADE optical telescope at Matera is owned by ASI and operated by e-GEOS. The telescope contributed in a LEO and GEO space debris campaign supporting the work of the Inter-Agency Space Debris Coordination Committee (IADC) (Telespazio 2017). The Sardinia Radio Telescope (SRT) is the result of a scientific and technical collaboration among three Structures of the Italian National Institute for Astrophysics (INAF): the Institute of Radio Astronomy of Bologna, the Cagliari Astronomy Observatory, and the Arcetri Astrophysical Observatory in Florence. Funding agencies are the Italian Ministry of Education, Universities and Research, the Sardinia Regional Government, and ASI. The manufacturing of the SRT mechanical parts and their assembly on-site was commissioned in 2003 to the company MTM (Germany). The final tests and acceptance of the instrument were performed in August 2012 (Tofanie 2008).

Space debris monitoring is part of the Italian Institute for Astrophysics (INAF) and Cagliari Astronomical Observatory research activity in the framework convention ASI/INAF “Space Debris—IADC activities support and SST preoperative validation.” In this framework, the INAF participation concerns the testing of the SRT’s operative capacities in the detection of signals scattered by space debris. ASI, INAF, and the Ministry of Defence have signed a framework agreement for the SST program. The agreement – which runs from June 2015 until end 2020 – foresees a Steering Committee for Space Surveillance and Tracking Activities (OCIS), responsible for coordinating the national activities in the European SST initiative and directing ASI as national entity representing Italy within the European SST Consortium (Telespazio 2017).

In January 2015, thanks to the cooperation with the Air Force’s IV Brigade, Telecommunication and Systems for Air Defence and Flight Assistance, a test was carried out in which the Selex ES (now Leonardo) RAT-31/DL FADR (Fixed Air Defence Radar) played the leading role. The system has become the backbone for the air surveillance of NATO countries, over the years. The test that successfully recorded the trajectory of several small satellites showed the advantages of using radar in the search of space debris. In comparison to the benefits of optical

telescopes, the radar has significant advantages. The testing campaign has given results that confirm the great potential of the FADR in this field, even opening the possibility of exploiting other Air Defence radar system networks across Europe (including numerous RAT-31/DLs installed in Austria, Poland, Hungary, the Czech Republic, Germany, and other countries) to provide satellite monitoring and surveillance services (Leonardo 2015).

---

## Spain

### Space and Security Budget

Spain had an estimated defense expenditure of €11.172 billion or 0.92% of GDP in 2018, below the NATO guideline of 2% of GDP. 19.3% of the 2018 estimated budget was allocated to equipment expenditure (NATO 2019). Spain has committed itself to “regularly increase” defense budgets to achieve the agreed objectives. In this sense, the government aims to increase its defense investment spending in the medium term “successively” so that it reaches 20% of the total expenditure on this matter and will increase the expenses dedicated to defense research and technology for approximate them to 2% of the total expenditure (The Diplomat 2017). Spain’s total space budget was estimated €354 million in 2018, including €293 million for civil activities and €61 million for defense. The budget driven by the contribution to ESA started to recover in 2016 after experiencing a decrease in 2013 followed by a 3-year stagnation. The 2018 budget grew by 18% compared to 2017 (Euroconsult 2019).

### Space and Security Activities and Programs

#### **Earth Observation (EO): Intelligence Surveillance-Reconnaissance (ISR)**

Spain has developed its own dedicated EO system. The Spanish *PNOTS (National Earth Observation Programme)* is a complete system, based on SEOSat/Ingenio and PAZ (Schrogl et al. 2015). The development of both satellites was established under the Space Strategic Plan 2007–2011 on flagship missions (CDTI 2008). With PNOTS Spain acquired a fully independent operational satellite remote sensing capability (Schrogl et al. 2015). PNOTS is funded and owned by the government of Spain. The project development of SEOSat/Ingenio is overseen by the European Space Agency (ESA) as a national contribution within the framework of Europe under a procurement assistance agreement signed between ESA and the Centre for the Development of Industrial Technology (CDTI) in 2007 (Space News 2018a). The National Institute of Aerospace Technology, INTA, is managing the ground segment of the two missions. The ground segment is being developed by an industrial consortium including Deimos, GMV, and Isdefe. The System will be operated from the ground station of Torrejon de Ardoz (Spain), which will be the primary control center of the mission and using Maspalomas (Canary Islands) as

backup station. The dual-use nature of the PAZ mission implies security constraints within its ground segment (SPIE 2017).

HISDESAT, together with INTA, is responsible for in-orbit operations and commercial operations of both satellites. Airbus Defence and Space Spain (formerly EADS CASA Espacio) is the prime contractor leading the industrial consortia of both missions. A major objective of PNOTS is to maximize the common developments and services and to share the infrastructure between both missions (whenever possible). Both missions will also contribute to the European Copernicus program. According to the contract, the ESA SEOSat/Ingenio project team must ensure that the European ground segment will allow the SEOSat/Ingenio system to become a candidate national mission contributing to Copernicus and to participate to the ESA third-party mission scheme within the EO multi-mission environment and therefore to support HMA (Heterogeneous Mission Access) services. SEOSat/Ingenio is the first Spanish Earth observation satellite financed by the Ministry of Economic Affairs, Industry and Competitiveness (formerly the Spanish Ministry of Industry) and built by a consortium of industries of the Spanish space sector with Astrium España (now Airbus Defence and Space Spain) as the prime contractor (with SENER, TASE, INDRA, GMV, and INTA) (Schrogl et al. 2015).

Ingenio is a satellite system with a foreseen 7-year operational lifetime in Sun-synchronous orbit (SSO) at 670 km. The payload consists of a multispectral imager (MS), a panchromatic imager (PAN), and an Ultraviolet and Visible Atmospheric Sounder (UVAS). SENER is responsible for the design, manufacturing, integration, alignment, and verification of the primary payload of the mission. The launch is scheduled for the first half of 2020 onboard a Vega launcher from Kourou (ESA 2014; SpaceWatch global 2019). PAZ will be one of the first satellites to combine Earth observation data with a sophisticated Automatic Identification System (AIS), which will allow to make the best possible monitoring of the world maritime environment. The expected operational lifetime is 5 and a half years. PAZ was launched in February 2018 by SpaceX from Vandenberg military base (SpaceX 2018).

HISDESAT is responsible for the launch and commercial operations of both satellites of the observation system in cooperation with the INTA, which is to provide ground control. Both satellites allow for Earth observation for multiple purposes: border control, intelligence, environmental monitoring, protection of natural resources, military operations, enforcement of international treaties, surface monitoring, city and infrastructure planning, monitoring of natural catastrophes, and high-resolution mapping, among many other (IDS 2014). The main center of the ground segment, located in the INTA, is completely installed with the integrated systems and in phase of interoperability tests. Spain's participation in the Pléiades program has allowed the national industry to reach industrial capabilities through the development of the ground segment for the Spanish Ministry of Defence (Spanish Ministry of Defence 2015a).

In the medium term, the amount, type, and cost of the PAZ satellite images necessary to cover the needs of the Ministry of Defence are expected to be assessed. In relation to the observation capacity, optics should analyze the options available



once the operational life of Helios is over. High-resolution optical images could be obtained through the kickoff of a program with industry participation without ruling out a possible cooperation of Spain in the optical component (CSO) of the MUSIS as a substitute for Helios. There are possibilities for a reorientation of employment of the facilities of the ground segment of the Pléiades, for a future national program or within the framework of the MUSIS program (Spanish Ministry of Defence 2015a).

### **Satellite Communications (SATCOM)**

*HISPASAT* was incorporated in 1989 to design, develop, manage, and deliver a commercial network capability as fleet operator in Ku band and Governmental services in X-band Satellite Communications System (SATCOM) for the Spanish government (Spanish Ministry of Defence 2015b). *HISPASAT* is owned by Abertis, a Spanish toll road company; SEPI, an industrial holding company; and Centre for the Development of Industrial Technology (CDTI) (Space News 2018b).

*HISDESAT* was incorporated in 2001 to define, develop, and operate new governmental SATCOM (Spanish Ministry of Defence 2015b). *HISDESAT* has been providing secure satellite communications services to the Spanish Ministry of Defence in support of all international missions of the Armed Forces, among others. It has also extended these services to other governments. *HISDESAT* services now include Earth observation, satellite communications, and AIS services through exactEarth (*HISDESAT* 2016). *HISDESAT* customers include the Spanish Ministry of Defence, Spanish Ministry of the Interior (CNI), Spanish Ministry of Economic Affairs, Industry and Competitiveness, the Spanish Regional Authorities, the Danish Ministry of Defence, Belgian Ministry of Defence, Norwegian Ministry of Defence, and US defense and intelligence agencies. *HISDESAT* operates SPAINSAT, Xtar-Eur, Paz and Ingenio (CDTI 2011; *HISDESAT* 2016). In 2007 an agreement was signed between the Ministries of Defence and Foreign Affairs to develop secure communications for the government's foreign activities. The project is based on two central hubs located at the Ministry of Foreign Affairs, with the entire network being connected through the geostationary satellites SPAINSAT and Xtar-Eur (IDS 2014). *HISDESAT*-operated secure communications services are provided by Ministry of the Interior to control borders between Spain, Portugal, and different African countries through the "Seahorse" program, strengthening security and illegal immigration control operations (IDS 2014).

The capacity of military satellite communications is covered by the service offered by the satellites *SPAINSAT*, as the main satellite, and Xtar-Eur as a redundant satellite. This set of satellites has a nominal life of 15 years, so, with its entry into operation in 2005 and 2006, the operational requirements of the Ministry of Defence are met until the year 2021. To meet this need, the Ministry of Defence and the companies *HISDESAT* and *HISPASAT* signed a framework agreement for the implementation of a satellite military communications system on 31 July 2001 Spanish Ministry of Defence (2015a). In May 2019, *HISDESAT* appointed Thales Alenia Space and Airbus to build two SPAINSAT Next Generation (NG) satellites for governmental communications that will replace the existing SPAINSAT and Xtar-Eur satellites. They will be launched in 2023, with an operational lifetime

15 years, aiming to guarantee the continuity of the secure communications services to the Spanish Ministry of Defence and Governmental Agencies using the current fleet (Space News 2019).

### **Positioning, Navigation, and Timing (PNT)**

Permanent GNSS network and associated services are organized at the level of autonomous communities/regions. HISDESAT holds a stake of 27% in exactEarth (HISDESAT 2016). Based in Canada, exactEarth is a leading organization in the field of global automatic identification system (AIS) vessel tracking, collecting the most comprehensive ship monitoring data and delivering the highest quality information to customers.

### **Space Situational Awareness (SSA)**

The Spanish Space Surveillance and Tracking (S3T) system provides services with two main objectives: to ensure the long-term availability of space infrastructures which are essential for the safety and security of worldwide citizens and to provide the best available information to governmental and civil protection services in the event of uncontrolled reentries of entire spacecraft or space debris thereof into the Earth's atmosphere. The SST services comprise collision risk assessment; the generation of conjunction data messages between objects in space; the detection and characterization of in-orbit fragmentations and collisions; and characterization and surveillance of uncontrolled reentries of space objects into the Earth's atmosphere (CDTI 2017).

The S3T system is currently contributing to the provision of these services by means of a national SST Operations Centre (S3TOC) and a set of ground-based sensors (S3TSN) which include optical surveillance and tracking telescopes and a surveillance radar. From a functional point of view, the S3TOC consists of a data-processing function, a sensor planning and tasking function, and a service provision function. The data-processing function is devoted to sensors' observation data processing, including correlation, orbit determination, and maintenance of a catalogue of space objects observed by the S3T sensors. The routine operations were initiated in July 2016. ESA is supporting CDTI in the development and procurement of the S3T system (CDTI 2017). Centu-1 is owned by Deimos, and it has been operationally contributing to the S3T system. It is used for surveillance, contributing to build up and maintain the S3T catalogue (CDTI 2017).

The Monostatic Space Surveillance Radar (MSSR) is a close-monostatic L-band radar, owned by the European Space Agency (ESA). It is located at the Santorcaz military naval base, about 30 km from Madrid (Spain). Through an agreement between the Spanish Ministry of Defence and ESA, the radar has been operational within the S3TSN since the end of the year 2016. The Ministry of Defence has participated in the selection of the site of the future advanced surveillance radar SST, as well as data policy and information security. In June 2015, it carried out the Transfer of the Operative Control of the Radar SSA of Santorcaz from ESA to the Air Force (CDTI 2017). The monostatic breadboard surveillance radar was developed within ESA's SSA Program. Following the completion of its development and

upon the Spanish government's request, the operation of the Radar was transferred on a loan basis to the Spanish Ministry of Defence for use in Spain's national SST activities. In relation to surveillance systems and spatial tracking, the Ministry of Defence supports the CDTI in the participation of Spain to the EU SST program (Spanish Ministry of Defence 2015a).

---

## The United Kingdom

### Space and Security Budget

Following the British vote to leave the European Union in 2016, the UK's economy has been experiencing political and economic uncertainty (Euroconsult 2019). UK covered an estimated defense expenditure of GBP 45.2 billion or 2.14% of GDP in 2018, above the NATO guideline of 2% of GDP. 22.4% of the 2018 estimated budget was allocated to equipment expenditure (NATO 2019). The UK government expenditure on space amounted to GBP694 million in 2018. 65% of the space budget was dedicated to civil space activities with top three expenditures in space science and exploration, Earth observation, and telecommunications. The UK's GBP 455 million civil space budget comprised of GBP 100 million invested in national programs, GBP 293 million contribution to ESA, and GBP 62 million contribution to EUMETSAT (Euroconsult 2019). The defense space expenditures equaled to GBP 240 million in 2018 primarily channeled toward military satellite communications (Skynet 5), while it is expected to grow for the future generation of the Skynet system and the British GNSS as an alternative to Galileo (Euroconsult 2019).

### Space and Security Activities and Programs

#### Earth Observation (EO): Intelligence Surveillance-Reconnaissance (ISR)

Traditionally, the UK has not put much emphasis on developing its own Earth observation satellites, because it has been relying on privileged access to relevant US assets (Schrogl et al. 2015). The UK Air and Space Doctrine explicitly mentions the relevance of environmental monitoring from space for security objectives (UK Ministry of Defence 2017).

UK Space Agency published in October 2013 a Strategy for Earth Observation from Space (2013–2016) in the context of the National Space Policy and the National Space Security Policy (April 2014). The strategy concentrates on civil EO requirements but recognizes that some civilian space systems could be dual-use in nature and be capable of supporting national security requirements (UKSA 2013).

In response to a recent parliamentary question, the Ministry of Defence elaborated on UK activities in the field of intelligence, surveillance, targeting, acquisition, and reconnaissance capability (ISTAR), stating that the activities are in line with the

Strategic Defence and Security Review “A Secure and Prosperous UK” of 23 November 2015. Intelligence, Surveillance, Target Acquisition and Reconnaissance and Information Systems and Services (ISS) are managed by the Ministry of Defence under a combined portfolio approach (UK Ministry of Defence 2012).

The Royal Air Force is strengthened by its ISTAR fleet in aerial reconnaissance. In the field of combat-aircraft ISTAR, the tactical imagery intelligence wing is an independent group force element, based at RAF Marham and covering a wide span of imagery intelligence missions. Its tasks include the exploitation of EO and infrared (IR) imagery, producing intelligence products in direct support of deployed operations (RAF 2012).

Resulting from the 2017 Defence Equipment Plan, the UK intends to spend GBP 5 billion through the ISTAR Operating Centre in the period 2017–2027. This investment includes spending on chemical, biological, radiological, and nuclear (CBRN) detection and countermeasures; electronic countermeasures; a range of equipment including communications, intelligence, surveillance, and reconnaissance; air defense; air traffic management; and tactical data links (UK Ministry of Defence 2018).

Civil spending in UK space activities is split between ESA, EUMETSAT, and national programs. In 2011, the UK invested GBP 21 million into NovaSAR-S, a low-cost SAR satellite developed by SSTL with maritime, forestry, flooding, and agriculture applications. The UK government provided GBP 21 million to assist in the development and launch of NovaSAR-S and will also benefit from access to the SAR data, significantly boosting the UK’s sovereign Earth observation capabilities for applications such as ship detection and identification, oil spill detection, forestry monitoring, and disaster monitoring, particularly flood detection and assessment (SSTL 2017). NovaSAR-S was launched in September 2018.

The Zephyr S next-generation High-Altitude Pseudo Satellite (HAPS) is a new variant of the Zephyr family of unmanned aerial vehicles (UAVs) owned by Airbus Defence and Space. Zephyr S is a production variant of Zephyr 8 demonstrator. The new variant is intended for a variety of military, security, and civil missions, including maritime surveillance, border patrol, intelligence, reconnaissance, navigation, satellite-like communications, missile detection, environmental surveillance, signals intelligence (SIGINT), continuous photo capturing, and humanitarian and disaster relief. Development on the Zephyr 8 HAPS program began in April 2014. The UK Ministry of Defence awarded a contract to Airbus Defence and Space for the production and operation of two Zephyr S solar-powered unmanned aircraft systems in February 2016. Airbus has partnered with four British small and medium enterprises, and two universities to help develop key technologies in aerostructures, energy storage, and propulsion for what it described as “the next generation of Zephyr” (AIN 2018). Combining solar power plus rechargeable batteries, the Zephyr S reached a world record for longest duration flight for an unmanned aircraft without refueling in January 2019. Just under 26 days, Zephyr S demonstrated that a long-term mission is feasible for a solely solar-electric, stratospheric-level unmanned aerial vehicle (UAV) flying above the weather and conventional air traffic (PowerElectronics 2019).

## Satellite Communications (SATCOM)

The UK's secure SATCOM capability is provided through a Private Finance Initiative (PFI) with Airbus, which is managed by Joint Forces Command. It provides a secure and resilient communications capability through the Skynet series of satellites and other SATCOM resources from other providers. UK partners and allies also use Skynet bandwidth, which bolsters collaborative ties, and, similarly, lost or degraded capabilities can be replaced by negotiating access to their space services. Commercial bandwidth can provide redundancy for military systems, but there are potential security risks if military communications are enabled by commercial satellites, which could also host foreign payloads. There are also risks in using commercial bandwidth because the terms of service provision could be significantly less than that provided through a dedicated military system (UK Ministry of Defence 2017).

Astrium Services (ASV) (now Airbus) is the service provider that has developed the widest array of SATCOMs for military and security purposes in a market-oriented pattern. With its Paradigm subsidiary, Airbus has built a commercial capacity under a long-term PFI contract with the UK Ministry of Defence, for the provision of military satellite communications services to 2022. Since 2003, Paradigm operates the five satellites of UK Skynet (Schrogl et al. 2015). In 2012, the UK government announced it would retake ownership of the Skynet system including the four spacecraft and ground segment at the end of the supply contract in 2022. The excess capacity is leased to other military customers in the USA, Canada, France, and NATO. Though the PFI with Airbus has permitted military requirements being met, the outsourcing may have decreased Ministry of Defence technical know-how and resources, hampering program management of the follow-up scheme which could be valued at 6 billion GBP (Schrogl et al. 2015).

A first element of a new British military satellite communications capability to replace the current *Skynet 5* network has been awarded to Airbus Defence and Space without a competition. Negotiations to complete the deal to supply the Skynet 6A satellite are ongoing. The Skynet 6 program is packaged into three elements: the stopgap spacecraft to be built by Airbus, a service delivery package to manage ground operations from 2022, and an enduring capability program to provide future communication system capacity beyond the end of the next decade. Ministry of Defence officials said that the default position on the two future, and larger, parts of the Skynet 6 program would be competitive. A third, smaller competition to appoint an acquisition partner to act as the customer's friend in the Skynet 6 procurement is also expected to move forward. Officials said they expect a competition to appoint a new service delivery partner to take over the running of the ground operations from 2022. The enduring capability is also in line to be competed as things stand. The final part of the Skynet 6 requirement will be the introduction of a future enduring communications capability, which will partly be provided by satellites (Defense News 2017). The Skynet 6A geostationary military communications satellite is scheduled to be operational by mid-2025 (Space News 2017b).

Resulting from the UK Defence Equipment Plan 2017, published on 31 January 2018, the UK plans to invest GBP 22.9 billion on Information Systems and Services

(ISS) in the period 2017–2027, including satellite communications. The UK foresees a change in its procurement strategy for the Future Beyond Line of Sight Strategic Communications program based on a PFI, the acquisition of satellites, and cost reduction for the existing Skynet 5 network (UK Ministry of Defence 2017).

The advanced multi-mode secure SATCOM modem called Proteus was initially developed by Airbus UK for the Ministry of Defence, specifically for use on the Skynet 5 system. Airbus is developing a stripped-down version that could be used outside the UK for partner countries. The Proteus modem offers robust protection against jamming and interception and is suitable for installation in fixed and mobile platforms through super high-frequency and extremely high-frequency SATCOM bands (Airbus 2018).

Almost all civil spending on satellite communications technology development is channeled via ESA.

### **Positioning, Navigation, and Timing (PNT)**

The UK has announced its plans to develop a national alternative to the EU's Galileo system (The Times 2018). The Government Office for Science procured a study into GNSS dependency rendered public in January 2018. The report sets out the findings of a review exploring the UK's dependency on GNSS covering threats and vulnerabilities, sector dependencies, mitigation strategy, and standards and testing. The Blackett report recommends measures to make UK critical services more resilient to disruption or loss of GNSS. Implementation of the Blackett recommendations is being overseen by a UK Cabinet Office Blackett Review Implementation Team (BRIG). The technical aspects of implementing the recommendations are being led by a (PNTTG), reporting to the BRIG (UK Government 2018).

Announced in May 2017, QinetiQ and Rockwell Collins aimed to develop under a new partnership next-generation multi-constellation Global Navigation Satellite System (GNSS) receivers. The focus would lie on developing a family of multi-constellation “open-service” GNSS receivers. Based on the high-level overview they have provided, the two companies are collectively looking to provide military and government aircraft operators with the ability to use and switch between use of existing and future GNSS constellations. Outside of aircraft GNSS development, QinetiQ and Rockwell Collins will also look to develop GNSS receivers designed to “reduce operational costs for ground troops, vehicles and high-dynamics GNSS-guided weapons” (Aviation Today 2017).

The British Isles continuous GNSS Facility (BIGF) supports research scientists with archived RINEX format GNSS data, metadata, and derivative products. This unique facility in the UK is hosted at the Nottingham Geospatial Institute – a center for related postgraduate teaching and research, at the University of Nottingham. BIGF was funded by the Natural Environment Research Council (NERC) from 2002 to 2018 and is now funded by United Kingdom Research and Innovation (UKRI) since 2018. The archive comprises data from GPS and GLONASS satellites, from a high-density network of around 160 continuously recording stations, located throughout mainland Britain, Northern Ireland, and Ireland (BIGF 2012).

Brexit does not prevent the UK as a third country from using the encrypted signal of Galileo provided that the relevant agreements between the EU and the UK are in place. Merely having access to PRS at some future date (as requested by the US and Norway) will not be good enough for London. The UK wants British companies to continue to participate in all aspects of the development and build of Galileo. Major contributions have been made by Surrey Satellite Technology Limited (SSTL), which has prepared the navigation payloads on every operational satellite in the sky; the UK arm of Airbus, which controls the satellites at its center in Portsmouth; and CGI (formerly Logica), which has been instrumental in designing the PRS itself (BBC 2018).

UKSA has written in May 2018 to all UK companies currently authorized to work on the secure elements of Galileo (including for instance SSTL, QinetiQ, and CGI), asking them to consult UKSA before taking on future contracts relating to the design and development of the program and its encrypted service. By reminding British companies that they need the express security clearance from ministers to engage in new contracts, London was essentially saying to Brussels that it has the power to stop those companies from handing over technical knowledge on PRS to firms in the EU-27 (BBC 2018). Yet, a UK GNSS will not add significantly new capabilities for defense as the UK will continue to have access to the precise signals of the American GPS and may access Galileo PRS after conclusion of a specific agreement for PRS access for third countries (as requested by the US and Norway). UK GNSS would only address *one* of the major losses in space power to the UK because of Brexit. It does not address being shut out of GOVSATCOM, EU SSA, and Copernicus (Defence in Depth 2018).

### **Space Situational Awareness (SSA)**

The UK holds three space surveillance systems, two radar systems and one optical system. The latter is a telescope managed by the British National Space Centre (BNSC) and named Starbrook. It is located in Cyprus and has an added experimental survey sensor since 2006. The two radar systems are the Fylingdales complex and the Chilbolton facility. The first is part of the US Space Surveillance Network and is operated by British armed forces. The second, CAMRa (Advanced Meteorological Radar), is managed by the Rutherford Appleton Laboratory and is mainly used for atmospheric and ionospheric research (European Parliament 2015).

The Daedalus experiment – part of the Space Situational Awareness Project in DSTL’s Space Programme – is exploring the effect on satellites of so-called Icarus “deorbit sails.” When deployed, the sail increases drag, causing a controlled descent into the Earth’s atmosphere where the satellite will burn up (UK Government 2017).

---

### **Concluding Remarks**

This chapter provides evidence of the trend toward increasing relevance for security and defense in national space and security programs. “Space and security,” both in its security from space and security in space aspects, are progressively contributing to

further integration of space activities. Traditionally, only civilian space activities including for instance Earth observation, telecommunications, human spaceflight, space transportation, and technology development were subject of cooperation projects at intergovernmental and supranational levels. Security or defense related space programs were kept at the national level or dealt with bilaterally or multilaterally in *ad hoc* cooperative programs. These trends demonstrate an evolution of the largest European countries' priorities from strictly civil-oriented applications to also encompassing security and defense ones, facilitating synergies based on the dual nature of space. National space programs with security or defense dimensions, in combination with the EU and ESA programs, demonstrate alignment toward the use of space for security and defense. To conclude, the increasing relevance of security and defense in Europe, to some extent, could be framed as the necessity for Europe to take its security and defense into its own hands *vis-à-vis* other global space powers. Hence, this appears to be a strong driver in the current geopolitical context.

**Disclaimer** The contents of this chapter and any contributions to the handbook reflect personal opinions and do not necessarily reflect the opinion of the European Space Agency (ESA).

---

## References

- AdV Website, Surveying authorities of the States of the Federal Republic of Germany, SAPOS – the German satellite positioning service. <http://www.adv-online.de/Products/SAPOS/>
- AIN (2018) Online, Airbus Zephyr Pseudo-satellite gets new funding, 19 January 2018. <https://www.ainonline.com/aviation-news/defense/2018-01-19/airbus-zephyr-pseudo-satellite-gets-new-funding>
- Air Force Technology Website, Military communications satellite systems, SATCOMBw Military Communications Satellite System. <https://www.airforce-technology.com/projects/satcombw-military-communications-satellite-system/>
- Airbus (2016) Airbus Defense & Space and Telespazio selected to provide satellite-based maritime surveillance service for the French Navy, 2 June 2016. <https://www.airbus.com/newsroom/news/en/2016/06/airbus-defence-and-space-and-telespazio-france-selected-to-provide-satellite-based-maritime-surveillance-service-for-the-french-navy.html>
- Airbus (2018) Network for the Sky – Secure networked airborne communications, July 2018. [https://www.nfts.airbus.com/wp-content/uploads/2018/07/A4\\_Brochure\\_V5\\_Final.pdf](https://www.nfts.airbus.com/wp-content/uploads/2018/07/A4_Brochure_V5_Final.pdf)
- Airbus (2020) Pléiades Neo well on track for launch mid-2020, 24 February 2020. <https://www.airbus.com/newsroom/press-releases/en/2020/02/pleiades-neo-well-on-track-for-launch-mid2020.html>
- Arianespace (2017a) Italian Space Agency and Italian Ministry of Defense choose Arianespace to launch COSMO-SkyMed Second-Generation (CSG) satellites manufactured by Thales Alenia Space on the occasion of the 34th French-Italian summit, 27 September 2017. <https://www.arianespace.com/press-release/italian-space-agency-and-italian-ministry-of-defense-choose-arianespace-to-launch-cosmo-skymed-second-generation-csg-satellites-manufactured-by-thales-alenia-space-on-the-occasion-of-the-34th-french/>
- Arianespace (2017b) OHB Italia, on behalf of the Italian Space Agency, and Arianespace sign contract to launch PRISMA Italian satellite, 19 June 2017. <https://www.arianespace.com/press-release/ohb-italia-on-behalf-of-the-italian-space-agency-and-arianespace-sign-contract-to-launch-prisma-italian-satellite/>
- ASI (2016) Strategic Vision Document 2016–2025. <https://www.researchitaly.it/en/projects/space-strategic-vision-2016-2025-document-published-by-asi/>



- Aviation Today (2017) QinetiQ, Rockwell Collins to develop new GNSS receivers, 26 May 2017. <https://www.aviationtoday.com/2017/05/26/qinetiq-rockwell-collins-develop-new-gnss-receivers/>
- BBC (2018) UK ups the ante on Galileo sat-nav project, 14 May 2018. <https://www.bbc.com/news/science-environment-44116085>
- BBK (2017) Federal Office for Civil Protection and Disaster Assistance, services for modern civil protection, September 2017. [https://www.bbk.bund.de/SharedDocs/Downloads/BBK/EN/Services\\_for\\_modern\\_civil\\_protection.pdf?\\_\\_blob=publicationFile](https://www.bbk.bund.de/SharedDocs/Downloads/BBK/EN/Services_for_modern_civil_protection.pdf?__blob=publicationFile)
- BIGF (2012) British Isles continuous GNSS Facility Folder, 2012
- Bird & Bird (2016) Satellite bulletin – February 2016: significant increase in French spending on military space programs, 26 February 2016. <https://www.twobirds.com/en/search?r=595be8b8-fac8-4244-a958-e39a6ef5dc14&s=51897736-c9a6-4562-a8ba-f54b70a0532d&nt=IndustryNews>
- Bloomberg (2019) OHB SE: satellite-based radar reconnaissance for Germany – OHB awarded additional contract for SARah project, 7 August 2019. <https://www.bloomberg.com/press-releases/2019-08-07/dgap-news-ohb-se-satellite-based-radar-reconnaissance-for-germany-ohb-awarded-additional-contract-for-sarah-project>
- Castagnetti C., Casula G., Capra A., Bianchi M. G., Dubbini M. (2010), Adjustment and transformation strategies of ItalPoS Permanent GNSS Network, Bulletin of Geodesy and Geomatics, vol. LXIX n. 2-3, p. 299-317, ISSN 0006-6710
- CDTI (2008) Centre for the Development of Industrial Technology, Spanish Earth Observation Programme, Presentation, 17 November 2008. [https://www.cdti.es/recursos/doc/Programas/Aeronautica\\_espacio\\_retornos\\_industriales/Agencia\\_Espacial\\_Europea/1245\\_251125112008103422.pdf](https://www.cdti.es/recursos/doc/Programas/Aeronautica_espacio_retornos_industriales/Agencia_Espacial_Europea/1245_251125112008103422.pdf)
- CDTI (2011) Centre for the Development of Industrial Technology, Spanish-Norwegian Space Industry Event, Presentation, May 2011. [https://www.cdti.es/recursos/doc/Programas/Aeronautica\\_espacio\\_retornos\\_industriales/Espacio/25260\\_1011101120111405.pdf](https://www.cdti.es/recursos/doc/Programas/Aeronautica_espacio_retornos_industriales/Espacio/25260_1011101120111405.pdf)
- CDTI (2017) Centre for the Development of Industrial Technology, Architecture of the Spanish Surveillance and Tracking System, ESA 7th European conference on space debris, 18–21 April 2017. <https://conference.sdo.esoc.esa.int/sites/default/files/Final%20programme%207th%20European%20Conference%20on%20Space%20Debris.pdf>
- CNES (2018) Appel a Idees Externe R&T Systemes Orbitaux, 26 June 2018. [https://rt-theses.cnes.fr/sites/default/files/users/2018-10946\\_APEL%20A%20IDEEES%20EXTERNE%20RT\\_2019-VF.pdf](https://rt-theses.cnes.fr/sites/default/files/users/2018-10946_APEL%20A%20IDEEES%20EXTERNE%20RT_2019-VF.pdf)
- Defense Aerospace (2004) Thales Appointed Prime Contractor for EUR 1.3 Billion Syracuse III Ground Segment Contract, 2 December 2004. [http://www.defense-aerospace.com/article-view/release/49797/thales,-alcatel-share-syracuse-iii-contract-\(dec.-3\).html](http://www.defense-aerospace.com/article-view/release/49797/thales,-alcatel-share-syracuse-iii-contract-(dec.-3).html)
- Defence in Depth (2018) Better the devil you know? Galileo, Brexit, and British Defence Space Strategy, 23 May 2018. <https://defenceindepth.co/2018/05/23/better-the-devil-you-know-galileo-brexite-and-british-defence-space-strategy/>
- Defense News (2017) Airbus scores British military satellite deal without competition, 31 July 2017. <https://www.defensenews.com/space/2017/07/31/airbus-scores-uk-military-satellite-deal-without-competition/>
- Defense News (2018a) Macron signs French military budget into law. Here's what the armed forces are getting, 16 July 2018. <https://www.defensenews.com/global/europe/2018/07/16/macron-signs-french-military-budget-into-law-heres-what-the-armed-forces-are-getting/>
- Defense News (2018b) Foreign governments are approaching French satellites in orbit, says space commander, 26 January 2018. <https://www.defensenews.com/space/2018/01/26/foreign-governments-are-approaching-french-satellites-in-orbit-says-space-commander/>
- Defense News (2018c) France tests radar to detect and track ballistic missiles, satellites, 23 March 2018. <https://www.defensenews.com/intel-geoint/sensors/2018/03/23/france-tests-radar-to-detect-and-track-ballistic-missiles-satellites/>
- Defense Aerospace (2017) Italian Space Agency and Italian Ministry of Defense Choose Arianespace to Launch COSMO-SkyMed Second-Generation (CSG) Satellites, 27 September

2017. <https://www.arianespace.com/press-release/italian-space-agency-and-italian-ministry-of-defense-choose-arianespace-to-launch-cosmo-skymed-second-generation-csg-satellites-manufactured-by-thales-alenia-space-on-the-occasion-of-the-34th-french/>
- DGA (2015) Direction générale de l'armement, Communication Satellites for European Defence and Security: French Perspectives, Presentation by P.-E. Schoumacher, 25 November 2015, Betzdorf, Luxembourg. <http://www.eu2015lu.eu/en/agenda/2015/11/25-seminaire-SatCom/index.html>
- DGA (2019a) Direction générale de l'armement, Notification de la deuxième étape du projet ARTEMIS de big data du ministère des Armées, 6 June 2019. <https://www.defense.gouv.fr/dga/actualite/notification-de-la-deuxieme-etape-du-projet-artemis-de-big-data-du-ministere-des-armees>
- DGA (2019b) Direction générale de l'armement, Syracuse IV, le ministère des armées commande la réalisation du segment sol, 17 June 2019. <https://www.defense.gouv.fr/english/dga/actualite-dga/2019/syracuse-iv-le-ministere-des-armees-commande-la-realisation-du-segment-sol>
- DLR (2016) New 3D world map – TanDEM-X global elevation model completed, 4 October 2016. [https://www.dlr.de/content/en/articles/news/2016/20161004\\_new-3d-world-map-tandem-x-global-elevation-model-completed\\_19509.html](https://www.dlr.de/content/en/articles/news/2016/20161004_new-3d-world-map-tandem-x-global-elevation-model-completed_19509.html)
- DLR (2017a) FireBIRD monitors forest fires in California, 19 December 2017. [https://www.dlr.de/content/en/articles/news/2017/20171219\\_firebird-monitors-forest-fires-in-california\\_25507.html](https://www.dlr.de/content/en/articles/news/2017/20171219_firebird-monitors-forest-fires-in-california_25507.html)
- DLR (2017b) Optical satellite downlinks at DLR – OSIRIS, Presentation, 12 July 2017. [https://artes.esa.int/sites/default/files/AM%2003\\_20170712\\_Fuchs\\_OpticalSatelliteDownlinksatDLR\\_final.pdf](https://artes.esa.int/sites/default/files/AM%2003_20170712_Fuchs_OpticalSatelliteDownlinksatDLR_final.pdf)
- DLR (2018) Earth observation for humanity – German Remote Sensing Data Center (DFD) at the DLR Earth Observation Center (EOC), Presentation, 6 March 2018
- DLR (2019) GESTRA space radar passes its first test, 29 November 2019. [https://www.dlr.de/content/en/articles/news/2019/04/20191129\\_latest-radar-technology.html](https://www.dlr.de/content/en/articles/news/2019/04/20191129_latest-radar-technology.html)
- DLR, Tandem-L – A Satellite Mission for Monitoring Dynamic Processes on the Earth's Surface. [https://www.dlr.de/content/en/downloads/publications/brochures/tandem-l-brochure\\_1663.pdf?\\_\\_blob=publicationFile&v=11](https://www.dlr.de/content/en/downloads/publications/brochures/tandem-l-brochure_1663.pdf?__blob=publicationFile&v=11)
- DLR Website, Institute of Communications and Navigation, GNSS Software Receiver. [https://www.dlr.de/kn/en/desktopdefault.aspx/tabid-2066/3255\\_read-9556/](https://www.dlr.de/kn/en/desktopdefault.aspx/tabid-2066/3255_read-9556/); GNSS HW-Simulator. [https://www.dlr.de/kn/en/desktopdefault.aspx/tabid-2066/3255\\_read-9429/](https://www.dlr.de/kn/en/desktopdefault.aspx/tabid-2066/3255_read-9429/)
- EARSC (2015) ASI and ISA strengthen the cooperation in the Earth Observation Field, 20 October 2015. <http://earsc.org/news/asi-and-isa-strengthen-the-cooperation-in-the-earth-observation-field>
- Earth Observation (EO) Portal Website, Sharing Earth Observation Resources, Satellite Missions, SAR-Lupe Mission. <https://directory.eoportal.org/web/eoportal/satellite-missions/s/sar-lupe>. Terra Mission. <https://directory.eoportal.org/web/eoportal/satellite-missions/t/terra>
- ESA (2014) SEOSAT/INGENIO, A Spanish High-Spatial-Resolution Optical Mission, Presentation, 2014
- Euroconsult (2019) Government space programs – benchmarks, profiles & forecasts to 2028, July 2019
- European Parliament (2006) Europe's space policies and their relevance to ESDP, June 2006. [https://www.files.ethz.ch/isn/26583/06\\_06\\_Space\\_Policy.pdf](https://www.files.ethz.ch/isn/26583/06_06_Space_Policy.pdf)
- European Parliament (2015) Space, sovereignty and European security – building European capabilities in an advanced institutional framework, 2014, 39. [https://www.europarl.europa.eu/RegData/etudes/etudes/JOIN/2014/433750/EXPO-SEDE\\_ET\(2014\)433750\\_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/etudes/JOIN/2014/433750/EXPO-SEDE_ET(2014)433750_EN.pdf)
- Fraunhofer (2018) Traveling into space – safely, quickly and cost-effectively, Press Release, 10 April 2018. <https://www.fraunhofer.de/en/press/research-news/2018/april/traveling-into-space-safely-quickly-and-cost-effectively.html>
- Fraunhofer Institute (2018) Space observation with radar to secure Germany's space infrastructure, Press Release, 23 March 2018. <https://www.fhr.fraunhofer.de/en/press-media/press-releases/2018/space-observation-with-radar-to-secure-germanys-space-infrastructure.html>

- French Joint Space Command (2016) SSA: first priority of French military space policy 2025, Presentation, Brigadier General Jean-Daniel TESTÉ, Commander, Joint Space Command, Tokyo, March 2016. <http://www.jsforum.or.jp/stableuse/2016/pdf/15.%20Teste.pdf>
- French Ministry of the Armed Forces (2012) Détecter un tir de missile balistique le plus tôt possible, 26 March 2012. <https://www.defense.gouv.fr/actualites/dossiers/l-espace-au-profit-des-operations-militaires/les-fonctionsspatiales-au-service-des-operations/detecter-un-tir-de-missile-balistique-le-plus-tot-possible>
- French National Assembly (2016) Commission de la défense nationale et des forces armées, 17 May 2016, Compte rendu n° 48. <http://www.assemblee-nationale.fr/14/cr-cdef/15-16/c1516048.asp>
- French Republic (2018a) PLF 2018 – Extrait du Bleu Budgétaire de la mission: Recherche et Enseignement Supérieur – Programme 191: Recherche Duale (civile et militaire), 2 October 2018. [https://www.performance-publique.budget.gouv.fr/sites/performance\\_publique/files/farandole/ressources/2019/pap/pdf/DBGPGM191.pdf](https://www.performance-publique.budget.gouv.fr/sites/performance_publique/files/farandole/ressources/2019/pap/pdf/DBGPGM191.pdf)
- French Republic (2018b) President of the French Republic, Bill on Military Planning 2019/2025, 19 January 2018. <https://www.defensenews.com/global/europe/2018/07/16/macron-signs-french-military-budget-into-law-heres-what-the-armed-forces-are-getting/>
- French Senate (2018) Projet de loi de finances pour 2018: Défense: Équipement des forces. [https://www.senat.fr/rap/a17-110-8/a17-110-8\\_mono.html](https://www.senat.fr/rap/a17-110-8/a17-110-8_mono.html)
- FRS (2015) Fondation pour la Recherche Stratégique, The European Space Surveillance and Tracking service at the crossroad, October 2015. <https://www.frstrategie.org/en/publications/defense-et-industries/european-space-surveillance-and-tracking-service-crossroad-2015>
- GPS World (2017) German Defense chooses Rockwell Collins NavHub system for GNSS, 14 September 2017. <https://www.gpsworld.com/german-defense-chooses-rockwell-collins-navhub-system-for-gnss/>
- GSA (2017) Galileo Public Regulated Service ready for action, 4 April 2017. <https://www.gsa.europa.eu/newsroom/news/galileo-public-regulated-service-ready-action>
- HISDESAT (2016) Spatial Resources in Ports of the Future, Presentation, April 2016. <https://www.aeit.es/sites/default/files/migrate/content/downloads/sebastiancatolfi.pdf>
- IAI (2003) Istituto Affari Internazionali, Space and Security Policy in Europe, November 2003, ESA Study. [https://www.esa.int/About\\_Us/Corporate\\_news/Space\\_and\\_security\\_policy\\_in\\_Europe](https://www.esa.int/About_Us/Corporate_news/Space_and_security_policy_in_Europe)
- IAI (2018) Istituto Affari Internazionali Boosting Defence Cooperation in Europe: an analysis of key military capabilities, June 2018. <https://www.iai.it/en/publicazioni/boosting-defence-cooperation-europe>
- IDS (2014) Spain Defence & Security Industry. <https://www.infodefensa.com/servicios/publicaciones/spain-defence-security-industry-2014.html>
- International Institute for Strategic Studies (2017) France and Germany: drivers of European defence-industrial cooperation, 18 December 2017. <https://www.iiss.org/blogs/military-balance/2017/12/european-defence>
- Janes.com (2017) OPTSAT-3000 gives Italy key space intelligence capability, 7 August 2017. <https://www.leonardocompany.com/en/press-release-detail/-/detail/optsat-3000-satellite-launch-earth-observation>
- La Tribune (2017) Observation spatiale: quand Allemagne se joue de la France, 8 December 2017, <https://www.latribune.fr/entreprises-finance/industrie/aeronautique-defense/observation-spatiale-quand-l-allemande-se-joue-de-la-france-760854.html>
- Le Figaro (2018) Florence Parly veut développer des capacités militaires spatiales, 21 June 2018. <https://www.lefigaro.fr/flash-actu/2018/06/21/97001-20180621FILWWW00047-florence-parly-veut-developper-des-capacites-militaires-spatiales.php>
- Leonardo (2015) Being protected from space RAT/31DL. <https://www.leonardocompany.com/en/news-and-stories-detail/-/detail/proteggersi-spazio-protected-from-space>
- Leonardo (2017) OPTSAT-3000 Earth observation satellite for Italy's Ministry of Defence is ready to be launched, 31 July 2017. <https://www.leonardocompany.com/en/press-release-detail/-/detail/optsat-3000-satellite-launch-earth-observation>

- Loizzo R (2016) The Prisma Hyperspectral Mission, living planet symposium 2016, 9–13 May 2016, Prague. [http://www.prima-i.it/images/Articoli/2016\\_Loizzo-et-al.pdf](http://www.prima-i.it/images/Articoli/2016_Loizzo-et-al.pdf)
- NATO (2019) Defence Expenditure of NATO Countries (2013–2019) Press Release, PR/CP (2019) 123, November 2019. [https://www.nato.int/nato\\_static\\_fl2014/assets/pdf/pdf\\_2019\\_11/20191129\\_pr-2019-123-en.pdf](https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_11/20191129_pr-2019-123-en.pdf)
- NGA (2015) NGA, Germany's Bundeswehr Geoinformation Centre sign geospatial data sharing agreement, 18 December 2015. <https://www.nga.mil/MediaRoom/News/Pages/NGA,-Germany%E2%80%99s-Bundeswehr-Geoinformation-Centre-sign-geospatial-data-sharing-agreement.aspx>
- OHB (2008) OHB subsidiary Kayser-Threde awarded contract for implementing the national earth observation mission EnMAP by the German Aerospace Center, 11 November 2008. <https://www.dgap.de/dgap/News/corporate/ohb-technology-ohb-subsiary-kayserthrede-awarded-enmap-contract/?newsID=369111>
- OHB (2013) OHB System AG awarded contract for the development and integration of the SARah radar satellite reconnaissance system for the German federal armed forces, 2 July 2013. <https://www.ohb-system.de/press-releases-details/ohb-system-ag-awarded-contract-for-the-development-and-integration-of-the-sarah-radar-satellite-reconnaissance-system-for-the-ge.html>
- OHB Website, Current Programs, Security, SAR-Lupe. <https://www.ohb-system.de/sar-lupe-english.html>; Current Programs, Communication, Heinrich Hertz. <https://www.ohb-system.de/heinrich-hertz-english.html>
- ONERA (2016) GRAVES: vers une surveillance spatiale française plus performante, Press Release, 12 December 2016. <https://www.onera.fr/en/node/95>
- PowerElectronics (2019) Solar-powered “Pseudo-satellite” aircraft logs first flight of 26 days, 10 January 2019. <https://www.powerelectronics.com/markets/automotive/article/21864274/solarpowered-pseudosatellite-aircraft-logs-first-flight-of-26-days>
- RAF (2012) Royal Air Force, the view from above – RAF ISTAR, 14 November 2012
- RTL INFO (2018) Les principales mesures de la loi de programmation militaire 2019–2025, 8 February 2018. <https://www.rtl.be/info/monde/france/les-principales-mesures-de-la-loi-de-programmation-militaire-2019-2025-994090.aspx>
- Sagath D, Papadimitriou A, Adriaensen M, Giannopapa C (2018) Space strategy and governance of ESA small member states. *Acta Astronaut* 142:112–120
- Satellite Observation (2016) A new German Space Policy? 28 December 2016. <https://satelliteobservation.net/2016/12/28/a-new-german-space-policy/>
- Schrogl K-U et al (eds) (2015) Handbook of space security: policies, applications and programs. Springer, New York
- Shephard (2016) Media, Airbus DS awarded COMSATBw contract, 10 March 2016. <https://www.shephardmedia.com/news/digital-battlespace/airbus-ds-keep-operating-comsatbw-satellites/>
- Space News (2017a) How close are high-altitude platforms to competing with satellites? 26 October 2017. <https://spacenews.com/how-close-are-high-altitude-platforms-to-competing-with-satellites/>
- Space News (2017b) U.K. military seeks to ride wave if commercial space innovation, 7 November 2017. <https://spacenews.com/u-k-military-seeks-to-ride-wave-of-commercial-space-innovation/>
- Space News (2018a) Morocco satellite launch could accelerate Spanish space efforts, 5 January 2018. <https://spacenews.com/morocco-satellite-launch-could-accelerate-spanish-space-efforts/>
- Space News (2018b) EUTELSAT completes 302 million EUR HISPASAT divestiture, 19 April 2018. <https://spacenews.com/eutelsat-completes-302-million-euro-hispasat-divestiture/>
- Space News (2019a) Airbus to build four imaging satellites for French space agency, mulls 20-plus constellation, 12 July 2019. <https://spacenews.com/airbus-to-build-four-imaging-satellites-for-french-space-agency-mulls-20-plus-constellation/>
- Space News (2019b) Airbus inks two-satellite deal with Spain's satellite operator Hisdesat, 6 May 2019. <https://spacenews.com/airbus-inks-two-satellite-deal-with-spains-satellite-operator-hisdesat/>
- SpaceWatch global (2019) Spain's SEOSAT/Ingenio Earth Observation Satellite Built by Airbus Ready for Pre-Launch Testing, June 2019. <https://spacewatch.global/2019/06/spains-seosat-ingenio-earth-observation-satellite-built-by-airbus-ready-for-pre-launch-testing/>

- SpaceX (2013) OHB signs contract for Germany's next-gen radar satellites, 2 July 2013. <https://spacenews.com/36091ohb-signs-contract-for-germanys-next-gen-radar-satellites/>
- SpaceX (2018) PAZ Mission, 22 February 2018. <https://www.spacex.com/news/2018/02/22/paz-mission>
- Spanish Ministry of Defence (2015a) Ministerio de Defensa, DGAM, Plan Director de Sistemas Espaciales, July 2015. <https://www.defensa.gob.es/Galerias/dgamdocs/plan-director-sistemas-espaciales.pdf>
- Spanish Ministry of Defence (2015b) Presentation on SECOMSAT – Spanish approach – present and future satcom for defence purposes, 25 November 2015. [http://www.eu2015lu.eu/en/agenda/2015/11/25-seminaire-SatCom/7\\_Roberto-PELAEZ-HERRERO.pdf](http://www.eu2015lu.eu/en/agenda/2015/11/25-seminaire-SatCom/7_Roberto-PELAEZ-HERRERO.pdf)
- SPIE (2017) Digital Library, SEOSAT/INGENIO: a Spanish high-spatial-resolution optical mission, 17 November 2017. <https://www.spiedigitallibrary.org/conference-proceedings-of-spie/10563/105632M/SEOSATINGENIO-a-Spanish-high-spatial-resolution-optical-mission/10.1117/12.2304151.full?SSO=1>
- Spiegel (2015) Spiegel Online, USA drängen auf Daten-Deal mit der Bundeswehr, 3 November 2015. <https://www.spiegel.de/politik/deutschland/bundeswehr-usa-draengen-auf-daten-deal-a-1060912.html>
- SSTL (2017) SSTL announces NovaSAR-S data deal with Australia's CSIRO, 26 September 2017. <https://www.sstl.co.uk/media-hub/latest-news/2017/sstl-announces-novasar-s-data-deal-with-australia->
- Telespazio (2017) Telespazio and TAS, Space Situation Awareness & Space Surveillance Tracking, 25 May 2017, Presentation. [http://www.cesmamil.org/wordpress/wp-content/uploads/2017/05/9-\\_Matarazzo-Brancati\\_-\\_Thales-Telespazio.pdf](http://www.cesmamil.org/wordpress/wp-content/uploads/2017/05/9-_Matarazzo-Brancati_-_Thales-Telespazio.pdf)
- Telespazio (2019) The first COSMO-SkyMed Second Generation satellite has been launched successfully, 18 December 2019. <https://www.telespazio.com/en/news-and-stories-detail/-/detail/171219-the-first-second-generation-cosmo-skymed-satellite-has-been-launched-successfully>
- Telespazio (2020a) Exploring the SICRAL programme. <https://www.telespazio.com/en/news-and-stories-detail/-/detail/171219-the-first-second-generation-cosmo-skymed-satellite-has-been-launched-successfully>
- Telespazio (2020b) The first COSMO-SkyMed Second Generation satellite has been launched successfully, 18 December 2019. <https://www.telespazio.com/en/news-and-stories-detail/-/detail/sicral-telespazio>
- Thales (2018) French Defence Procurement Agency Selects Thales and Sopra Steria to compete for Artemis an innovation partnership for the Armed Forces Ministry's Big Data Platform, Press Release, 11 April 2018. <https://www.thalesgroup.com/en/worldwide/security/press-release/french-defence-procurement-agency-selects-thales-and-sopra-steria>
- The Diplomat (2017) Spain adheres to EU's common framework of defence and security, 11 November 2017. <https://thediplomatinspain.com/en/spain-adheres-to-eus-common-framework-of-defense-and-security/>
- The Times (2018) UK will launch satellite system to rival EU's Galileo, 2 May 2018. <https://www.thetimes.co.uk/article/uk-will-launch-satellite-system-to-rival-eu-s-galileo-8127sl8fc>
- Tofanie G (2008) Status of the Sardinia Radio Telescope project, proceedings of the international society for optical engineering, January 2008
- UK Government (2017) DSTL Scientists tackle growing problem of space junk, press release, 24 July 2017. <https://www.gov.uk/government/news/dstl-scientists-tackle-growing-problem-of-space-junk>
- UK Government (2018) Satellite-derived time and position: Blackett review – Review exploring our dependency on global navigation satellite systems (GNSS), 30 January 2018. <https://www.gov.uk/government/publications/satellite-derived-time-and-position-blackett-review>
- UK Ministry of Defence (2012) The Defence Equipment Plan 2012. <https://www.gov.uk/government/publications/the-defence-equipment-plan-2012>

- UK Ministry of Defence (2017) Joint Doctrine Publication 0-30 (JDP 0-30) – UK Air and Space Power, second edition, December 2017. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/668710/doctrine\\_uk\\_air\\_space\\_power\\_jdp\\_0\\_30.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/668710/doctrine_uk_air_space_power_jdp_0_30.pdf)
- UK Ministry of Defence (2018) The Defence Equipment Plan 2017, 31 January 2018. <https://www.gov.uk/government/publications/the-defence-equipment-plan-2017>
- UKSA (2013) UKSA, Strategy for Earth Observation from Space 2013–16, October 2013. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/350655/EO\\_Strategy\\_-\\_Finalv2.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/350655/EO_Strategy_-_Finalv2.pdf)
- UNCOPUOS (2017) General presentation of French activities and views for the long-term sustainability of outer space, in relation with the implementation of the first set of guidelines (A/71/20, Annex), A/AC.105/C.1/2017/CRP.26, 3 February 2017. [https://www.unoosa.org/res/oosadoc/data/documents/2017/aac\\_105c\\_12017crp/aac\\_105c\\_12017crp\\_26\\_0\\_html/AC105\\_C1\\_2017\\_CRP26E.pdf/](https://www.unoosa.org/res/oosadoc/data/documents/2017/aac_105c_12017crp/aac_105c_12017crp_26_0_html/AC105_C1_2017_CRP26E.pdf/)



# Space and Security Programs in Medium-Sized European Countries

# 63

Ntorina Antoni, Christina Giannopapa, and Maarten Adriaensen

## Contents

Introduction .....	1266
Austria .....	1267
Space and Security Budget .....	1267
Space and Security Activities and Programs .....	1267
Belgium .....	1268
Space and Security Budget .....	1268
Space and Security Activities and Programs .....	1269
The Netherlands .....	1271
Space and Security Budget .....	1271
Space and Security Activities and Programs .....	1272
Norway .....	1275
Space and Security Budget .....	1275
Space and Security Activities and Programs .....	1276
Sweden .....	1279
Space and Security Budget .....	1279
Space and Security Activities and Programs .....	1280
Switzerland .....	1281
Space and Security Budget .....	1281
Space and Security Activities and Programs .....	1282
Concluding Remarks .....	1284
References .....	1285

---

N. Antoni (✉)  
Eindhoven University of Technology, Eindhoven, The Netherlands  
e-mail: [ntorina.antoni@gmail.com](mailto:ntorina.antoni@gmail.com)

C. Giannopapa · M. Adriaensen  
European Space Agency (ESA), Paris, France  
e-mail: [christina.giannopapa@esa.int](mailto:christina.giannopapa@esa.int); [maarten.cm.adriaensen@gmail.com](mailto:maarten.cm.adriaensen@gmail.com)

---

**Abstract**

This chapter presents the space and security programs of medium-sized European countries and indicates their main priorities and trends. In particular, the current chapter addresses the different types of space activities and programs in the fields of Earth observation (EO), Intelligence-Surveillance-Reconnaissance (ISR), Satellite Communication (SATCOM), Positioning, Navigation, and Timing (PNT), and Space Situational Awareness (SSA). The countries presented are Austria, Belgium, the Netherlands, Norway, Sweden, and Switzerland.

---

**Introduction**

The increased need for security in Europe and for Europe's space activities has led to several activities and programs developed by European countries in aerospace and defense. The main actors in Europe engaging in space and security activities are the European countries, the European Union (EU), and the European Space Agency (ESA). ► [Chap. 61, "Institutional Space Security Programs in Europe"](#) in this handbook describes how security and defense policies are progressively and gradually being supported by space programs of the EU, ESA, and the European Defence Agency (EDA), with the North Atlantic Treaty Organization (NATO) is also getting gradually involved. The European countries' space security policies are to a large extent determined by national needs and priorities, as explained in ► [Chap. 25, "Space and Security Policy in Selected European Countries."](#) In addition, policies are influenced by the space and security governance and their participation in relevant organizations as explained in ► [Chap. 23, "Strategic Overview of European Space and Security Governance."](#)

As such, the various space security activities and programs are to a large extent determined by national needs and priorities as well as participation to space and security-relevant organizations, including the EU and ESA. The current chapter addresses the space and security budgets, activities, and programs of selected European countries in Earth observation (EO), Intelligence-Surveillance-Reconnaissance (ISR), Satellite Communication (SATCOM), Positioning, Navigation, and Timing (PNT), and Space Situational Awareness (SSA). The European countries may be distinguished not only based on their membership to the space and security-related organizations but also based on their space budget. In the absence of an official grouping of these countries, their ESA annual budget and their defense expenditure as share of their growth domestic product (GDP) are used to classify them into three groups (Sagath et al. 2018).

The group presented in this chapter includes Member States with a GDP between €350 billion and €1.2 trillion and an annual ESA space budget (2018 ESA budget) typically between €50 and €200 million: Austria, Belgium, the Netherlands, Norway, Sweden, and Switzerland (Sagath et al. 2018). This chapter complements the chapters on the largest and smaller European countries presented in the corresponding chapters of the Handbook. The content is up to date until January 2019.



## Austria

### Space and Security Budget

Austria's defense budget was estimated at €2.26 billion in 2018 (0.58% of GDP) and €2.29 billion in 2019 (0.57% of GDP), and is expected to rise to €2.42 billion in 2020 (0.58% of GDP). The figures of the budgetary framework 2018/2019–2022 will increase, and budgetary regulations will be adapted to support the National Defence Plan 21.1 (OSCE 2018). The Austrian government expenditure for space-related activities amounted to €67.9 million in 2018 (Euroconsult 2019). The Austrian contribution to ESA in 2018 was €47 million. Austria is a member of the European Organization for the Exploitation of Meteorological Satellites (EUMETSAT), with a contribution in 2018 of €12 million. The main pillars of the Austrian space activities are the Austrian contributions to the programs of ESA and EUMETSAT, the contributions to EU space activities and the national space program (Euroconsult 2019). No military space budget has been identified by Euroconsult.

### Space and Security Activities and Programs

The Austrian Space program is in principle based on two national programs that have been carried out since 2002: the Austrian Space Applications Programme (ASAP) and the Austrian Radio Navigation Technology and Integrated Satnav services and products Testbed (ARTIST). Through ASAP, Austrian research institutions as well as commercial enterprises have been supported in their efforts in conducting space science and exploration and in developing space technologies, products, and services. ARTIST is intended as an Austrian testbed for navigation applications. Possible future applications and services of the European satellite system GALILEO have been tested and evaluated through demonstration projects with respect to their innovative character and technical and economic benefits (BMVIT 2017).

### Earth Observation (EO) – Intelligence – Surveillance-Reconnaissance (ISR)

The Technical University of Vienna, the *Zentralanstalt für Meteorologie und Geodynamik* (ZAMG), and private sector actors established in 2014 the Earth Observation Data Centre for Water Resources Monitoring (UN SPIDER 2014). Austria participates to the French Pléiades program. Moreover, Austria is part of the Copernicus program in the frame of the EU and ESA. Austria's contribution to ESA's optional Earth observation programs amounted to €9.63 million in 2018 (Euroconsult 2019). Further, Austria is a member of the following international organizations: the European Centre for Medium-Range Weather Forecasts (ECMWF); the Global Earth Observation System of Systems (GEOSS); the CEOS (Committee on Earth Observation Satellites); and the WMO (World Meteorological Organization).

### **Satellite Communications (SATCOM)**

The Technical University in Graz has a dedicated Institute of Communication Networks and Satellite Communications. The Research Priorities on Satellite and terrestrial broadband communication are Internet via satellite; digital TV and interactive Internet applications; 40 GHz fixed-broadband wireless access; tele-education, telemedicine, and emergency communications as applications; communications systems for air platforms (TU Graz Website). Additionally, sharing of national SATCOM assets is facilitated through the EDA EU SATCOM Market and the EDA Project Team on Satellite Communications, while technology development is facilitated through ESA. Austria participates in satellite communication activities through ESA's optional ARTES programs, with a budget of €8.12 million for 2018 (Euroconsult 2019). Further, Austria is a member of the International Maritime Organization (IMO) Global Maritime Distress and Safety System.

### **Positioning, Navigation, and Timing (PNT)**

Austria carries out space research and development at national level: TACTIC (Creating Awareness of Galileo Public Regulated Service-PRS at Critical Infrastructures) and PRS-Austria. PRS Austria studied the impact and countermeasures of Austrian PRS application scenarios in GNSS denied environments (TU Graz Website). Moreover, Austria participates in the optional ESA navigation programs in conjunction with the EU EGNOS/Galileo flagship program. Additionally, Austria is part of the COSPAS-SARSAT international satellite system for search and rescue.

### **Space Situational Awareness (SSA)**

The Satellite Laser Ranging Station at the Lustbühel Observatory in Graz is a world leading research institute in space surveillance and tracking (BMVIT 2017). Austria's contribution to the optional SSA program at ESA was €0.55 million in 2018 (Euroconsult 2019).

---

## **Belgium**

### **Space and Security Budget**

Belgium has an estimated defense expenditure of €4.1 billion or 0.93% of GDP in 2018, below the NATO guideline of 2% of GDP. From 2019 on, the budgetary path followed a progressive and linear growth expected to reach a defense effort of 1.3% of the GDP by 2030 (NATO 2019). The Belgian Federal Parliament approved in May 2017 a law authorizing €9.2 billion of investments for the military until 2030, including remotely piloted aircraft systems (RPAS), airplanes, and frigates (Belgian Parliament 2017). The Belgian government expenditure for civil space-related activities amounted to €219 million in 2018, with the largest contribution of €47 million going to ESA (Euroconsult 2019). An amount of €14.5 million was allocated to EUMETSAT in 2018 (EUMETSAT 2018). The Law from May 2017 approving

€9.2 billion in military investments includes satellite communications (SATCOM), Imagery intelligence (IMINT), and intelligence, surveillance, target acquisition, and reconnaissance (ISTAR) (Belgian Parliament 2017). Accordingly, the decision of the Ministry of Defense to join the CSO French reconnaissance program has boosted the defense space expenditures (Belgian Ministry of Defence 2016).

## Space and Security Activities and Programs

### **Earth Observation (EO) – Intelligence-Surveillance-Reconnaissance (ISR)**

STEREO III (Support to the Exploitation and Research in Earth Observation) is the ongoing Belgian program for remote sensing research. The thematic research priorities include global monitoring of vegetation and evolution of terrestrial ecosystems; management of the environment on a local and regional scale; interaction between change in land cover and climate change; epidemiology and humanitarian aid; security and risk management (BEOP Website). Furthermore, the Flemish Institute for Technological Research (VITO) is involved in the processing of remote sensing imagery. VITO is charged with the payload data ground segment of the PROBA-V mission. VITO develops and operates Earth observation systems that are used to collect data about population growth, urban development, agriculture, the forestry industry, and natural disasters (VITO Website). In addition, the VEGETATION program is the result of a collaboration among Belgium, France, Italy, Sweden, and the European Commission. The system consists of two observation instruments, SPOT 4 and SPOT 5 satellites that study the state of vegetation at a global level and track its spatial and temporal evolution. One of the most important contributions of Belgium is the funding and the hosting of the Image Processing Centre at VITO Mol (BELSPO Website).

Belgium takes part in the NAOS (National Advanced Optical System) Program with Luxembourg. Luxembourg is benefiting from Belgian expertise in the frame of its Earth observation program NAOS, which will provide Luxembourg along with EU and NATO partners with additional ISR capabilities. LUXGOVSAT will become the operator and the Belgian Ministry of Defense will support payload operations for LUXGOVSAT (SpaceNews 2017). Belgium also participates in the French Pléiades program, the Multinational Space-based Imaging System (MUSIS) program, and the Hélios-II program. According to the strategic vision for Defence (2016–2030), Belgium aims to invest €45.7 million in the French *Composante Spatiale Optique* (CSO) program (Belgian Ministry of Defense 2016). Moreover, Belgium is part of the Copernicus program in the frame of the EU and ESA. Belgium participates in ESA's optional Earth observation programs, with a budget of €31 million for 2018 (Euroconsult 2019). Further, Belgium is a member of the following international organizations: ECMWF, GEOSS, CEOS, and the WMO.

### **Satellite Communications (SATCOM)**

Since 2006, Belgium leases X-band satellite communications capability through a multiyear contract for indeterminate duration from Hisdesat for X-band capacity of

XTAR-EUR & SPAINSAT as C-band communications were insufficient to meet current and future needs. The satellite communications provide the required link between the operational center of the defense staff with military detachments overseas through the mobile stations and the BEMILSATCOM ground station in Marche-en-Famenne. Belgium leases communications from EUTELSAT and INTELSAT since 1999 (Skywin 2015). In addition, NEWTEC offers state-of-the-art commercial off-the-shelf satellite communications technology and solutions for the government and defense market. The Newtec Dialog VSAT platform is a scalable, flexible, and efficient multiservice satellite communications platform that allows network operators and satellite service providers to build and adapt their networks easily and in an affordable way as government and defense operations evolve (NEWTEC 2018).

In addition, Thales is a long-standing partner of the Belgian Armed Forces, supplying tactical communication systems and a variety of onboard sensors for armored vehicles, ships, helicopters, and unmanned aerial vehicles (UAV). Thales group, based in Belgium, provides encryption systems and secures satellite communications for NATO. Belgium is a partner of the Wideband Global SATCOM-9 (WGS), through the sharing of Luxembourg's allocation in the WGS system (SpaceNews 2017). Moreover, Belgium is supporting Luxembourg on governmental satellite communications. LuxGovSat's first satellite, GovSat-1 was launched in January 2018 and operates in X-band and military Ka-band to provide secure and assured Government services for EU and NATO. Belgium and Luxembourg have also cooperated in the frame of PACIS-1 (ESA 2017). Belgium is a member of the IMO Global Maritime Distress and Safety System.

Additionally, sharing of national SATCOM assets is facilitated through EDA EU SATCOM Market and the EDA Project Team on Satellite Communications, while technology development is facilitated through ESA. Belgium participates in satellite communication activities through ESA's optional ARTES programs, with a budget of €20.8 million for 2018 (Euroconsult 2019).

### **Positioning, Navigation, and Timing (PNT)**

The first continuously operating GPS reference station in Belgium was installed in 1992 by the Royal Observatory of Belgium (ROB). Over the years, several additional tracking stations have been installed in Belgium. The ROB network was extended, but also each of the regions (Flanders, Wallonie, and Brussels) installed their own network of permanent GPS stations. The ROB has installed several continuously operating reference stations in Belgium. The primary goal of these stations is the integration of Belgium to international reference systems (ROB Website).

Moreover, the Redu Centre in Belgium has expanded to host Galileo's in-orbit test centre and a Galileo sensor station. The main purpose is to verify the performance of the payloads on the four Galileo In-Orbit Validation (IOV) satellites, including radio frequency and baseband parameters, easurements (GPS World 2018). Most of Belgium's military capabilities will continue to rely on GPS in the near term, although alternative Global Navigation Space System (GNSS)

capabilities are being pursued to improve resilience. Further, Belgium participates in the optional ESA navigation programs in conjunction with the EU EGNOS/Galileo flagship program. Additionally, Belgium is part of the COSPAS-SARSAT international satellite system for search and rescue.

### **Space Situational Awareness (SSA)**

The PROBA2 Science Centre (P2SC), located at the Royal Observatory of Belgium in Brussels, oversees scientific operations and data processing for ESA's PROBA2 spacecraft. The P2SC has a science operations center, where instrument observing plans are devised with support also by ESA's Spacecraft Operations Centre in Redu. Finally, the P2SC serves as the main site for coordination of the PROBA2 Science Working Team (Proba2 Science Center Website).

In February 2017, BELSPO entered into an agreement with USSTRATCOM to share SSA services and information. The arrangement enhances awareness within the space domain and increases the safety of spaceflight operations. Belgium joined other nations (the UK, the Republic of Korea, France, Canada, Italy, Japan, Israel, Spain, Germany, Australia, and the United Arab Emirates), intergovernmental organizations (ESA and EUMETSAT), and more than 50 commercial satellite owner/operator/launchers already participating in SSA data-sharing agreements with USSTRATCOM (US Strategic Command 2017).

In addition, Belgium hosts the ESA SSA Space Weather Coordination Centre (SSCC) at the Space Pole. The SSCC coordinates the provision of space weather services available either at the SWE Data Centre located in Redu or at federated sites. The SSCC monitors the service network and provides the first-level user support with the help of scientific experts in the topics of solar weather, space radiation, ionospheric weather and geomagnetic conditions (ESA SSCC Website). The SSCC is operated by a Belgian consortium on behalf of ESA's SSA program Office. Belgium's budget for the optional ESA SSA program was €1.6 million in 2018 (Euroconsult 2019).

---

## **The Netherlands**

### **Space and Security Budget**

The Dutch economy continues to grow faster than the average in the eurozone, with a GDP growth at 2.7% in 2018 compared to the previous year, mostly driven by domestic demand (Euroconsult 2019). The Netherlands defense expenditure equaled to €9.45 billion or 1.36% of GDP in 2018, below the NATO guideline of 2% of the GDP (NATO 2019). The Netherlands had an estimated space budget of €150 million in 2018 covering all public civil and defense expenditure at national and international level. This amount comprises of €91 million contribution to ESA (26% increase compared to 2017), €24.8 million contribution to EUMETSAT, and €34 million to the Dutch National Program. The space defense expenditure for the field of telecommunications was €2 million in 2018 (Euroconsult 2019).

## Space and Security Activities and Programs

### **Earth Observation (EO) – Intelligence-Surveillance-Reconnaissance (ISR)**

The Netherlands has provided as in-kind contribution to Sentinel-5P a measurement instrument called *Tropomi*, which conducts research/monitoring of the atmosphere. Sentinel-5P was launched on 13 October 2017 from Plesetsk. The Dutch industry and public research organizations worked together for 7 years on the Tropomi development, spending an estimate of €133 million on the project. The project was funded and supported by the Ministry of Economic Affairs and Climate, the Ministry of Infrastructure and Water Management, and the Ministry of Education, Culture and Science. The Dutch government invested €98 million with the remainder financed by ESA. NSO worked together with Royal Dutch Meteorological Institute (KNMI), the Netherlands Organization for Applied Scientific Research (TNO), and the Dutch national expertise institute for scientific space research (SRON). Airbus Defence and Space Netherlands was the prime contractor (Dutch Government 2017a).

The *Scanning Imaging Absorption Spectrometer for Atmospheric Cartography (SCIAMACHY)* instrument on board ESA's Envisat mission (2002–2012) was a spectrometer that could measure a wide range of the electromagnetic spectrum. It was able to support research into the composition of the atmosphere. Absorptions in this spectrum provide information about the concentration of trace gases in the atmosphere, which in turn are a measure for air quality and climate change. The SCIAMACHY instrument was jointly realized by the Netherlands, Germany, and Belgium (NSO Website).

The NSO provides no-cost access to raw, unprocessed satellite data from several optical and SAR sensors through its Satellitedataportaal (satellite data portal). NSO purchased such data, financed by the Ministry of Economic Affairs and the Directorate of Infrastructure and Water Management, and made it publicly available to everybody in the Netherlands. Since 2015, a part of the satellite data has been made available free of charge via the European Copernicus program (NSO Website).

In 2012, the NSO entered into a 3-year agreement with MDA to license *RADARSAT-2* data with coverage over the Netherlands. The standard mode, dual-polarized data is processed and delivered to the Satellietdataportaal where Dutch users can access the data. During the contract term, the NSO expects to acquire close to 600 Standard, dual-polarized *RADARSAT-2* images of the Netherlands and its surrounding waterways. The focus of the work by the NSO and the Dutch geospatial community is on agricultural and interferometric synthetic aperture radar (InSAR) applications (MDA 2015).

Additionally, the Dutch Geodata for Agriculture and Water (G4AW) program stimulates sustainable food production, a more efficient use of water in developing countries, and aims to alleviate poverty by enhancement of sustainable economic growth and self-reliance in the G4AW partner countries. G4AW provides a platform for partnerships of private and public organizations. Together they provide food producers with relevant information, advice, or financial products. G4AW is a

program of the Dutch Ministry of Foreign Affairs with policy priorities for food security and water, which is executed by the NSO (NSO Website).

In September 2015, the Ministry of Justice and Security launched the innovation program Satellite applications in a so-called triple helix collaboration with external partners such as NSO, TNO, and The Hague Security Delta. Implementing organizations within the Ministries of Defence; Finance, Infrastructure, and the Environment; and Social Affairs and Employment have joined components of this program. The aim is to develop innovative products and services based on public-private partnerships to develop and implement satellite technology in security and justice. In addition, the Ministry of Justice and Security wants to gain experience with the use of new technology. In this program furthermore, attention is also paid to the risks of dependence on satellite technology and the protection of privacy (NSO 2016).

Moreover, *Ozone Monitoring Instrument (OMI)* is an Earth observation instrument, commissioned by the Netherlands and Finland, which measures the concentration of ozone and other trace gases in our atmosphere. OMI maps the worldwide ozone concentration daily. This information is useful for the prediction of the intensity of ultraviolet radiation and smog formation. The OMI instrument is part of the EOS-AURA satellite, built under the responsibility of NASA and launched in 2004. OMI was developed by Airbus Defence and Space Netherlands (then called Dutch Space) and TNO. The KNMI was scientific leader of the project and SRON was also closely involved in the project. OMI derives its heritage from NASA's Total Ozone Mapping Spectrometer (TOMS) instrument and the ESA Global Ozone Monitoring Experiment (GOME) instrument (on the ERS-2 satellite). OMI measures criteria pollutants such as O<sub>3</sub>, NO<sub>2</sub>, SO<sub>2</sub>, and aerosols (Airbus Defence & Space OMI Website).

Further, the Netherlands is part of the Copernicus program in the frame of the EU and ESA. The Netherlands contribution to ESA's optional Earth observation programs amounted €12.4 million for 2018 (Euroconsult 2019). The Netherlands is a member of the following international organizations: ECMWF, GEOSS, CEOS, and the WMO.

### **Satellite Communications (SATCOM)**

The Dutch Ministry of Defense has awarded a contract to Thales to supply naval satellite communications (SATCOM) terminals on the four ocean patrol vessels that are being built for the Royal Netherlands Navy. Under the contract, the company will deliver a complete SATCOM solution including state-of-the-art dual-band stabilized antenna, with civilian SATCOM Ku-band and military X-band. The SATCOM solution incorporates leading-edge multiband and stabilization capabilities, using multiple transmission systems, and ensuring perfect onboard integration. With the naval satellite communications terminals, the ocean patrol vessels will be able to communicate over secure, high-bandwidth satellite links with other national and allied force elements. The SATCOM solution is already in service in several NATO countries, including France, Belgium, and Norway (Naval Technology 2009).

The Ministry of Defense has a program called *Militaire Satelliet Communicatie lange termijn* (Defensiebreed) – MILSATCOM. The project covered a total cost of €132.3 million between 2007 and 2019 and is aimed at guaranteeing high-frequency

satellite capacity, establishing ground stations in the Netherlands and Curacao as well as procuring mobile ground segment. The Netherlands intends to replace their MILSATCOM ground terminals by 2020 (Dutch Ministry of Defense 2017).

In November 2017, the Royal Netherlands Air Force (RNAF) and the Netherlands Aerospace Centre (NLR) signed two agreements. These agreements contribute to RNAF's strategic ambition to use information-driven functionalities to improve and accelerate its response to potential military threats. The first agreement concerns the development and launch of a so-called nanosatellite for demonstration of technological possibilities relevant for staging military operations. The second agreement concerns the renewal of the existing covenant between RNAF and NLR aimed at joint knowledge building in the field of military air and space operations (NLR 2017a).

The nanosatellite, named "Brik-II" is a 6 U CubeSat, is expected to be launched in 2020. The main tasks of Brik-II are navigation, communication, and Earth observation. NLR is responsible for the instrument detecting radio waves from sources including radar installations. This will enable RNAF to better map its surroundings. NLR not only developed the idea for the instrument but designed and constructed it as well. NLR is also responsible for "ground processing," which involves the collected raw data being converted into data with military relevance. The nanosatellite's foremost purpose is to acquire knowledge about the space domain and to prove military-relevant applications. The nanosatellite will be a precursor to future satellites, for which both the acquired technological knowledge and operational experience will be used to develop the next generation of Dutch military satellites. The second agreement concerns the renewal of the covenant between RNAF and NLR relating to military air and space operations. Its purpose is to jointly develop this field of knowledge and align the strategies of the two parties (NLR 2017a).

The RNAF's strategy is to develop capabilities to enable it to carry out military operations from the air and from space. Parallel to this, RNAF will undergo a transformation to become an information-driven and agile air force organization with advanced operational capabilities. Obtaining the right volume of intelligence at the right time plays a central role in this. Getting hold of the right data before an enemy does will enable RNAF to increase its operational pace and improve its effectiveness and thereby to respond faster and better than its opponent (NLR 2017a).

The Netherlands is a founding member along with Canada, Denmark, Luxembourg, and New Zealand of the WGS-9 (part of the US-led WGS system). WGS-9 was launched in March 2018. The contribution gives the countries access to the WGS military communications system (Dutch Air Force 2017). The Netherlands is a member of the IMO Global Maritime Distress and Safety System. Additionally, sharing of national SATCOM assets is facilitated through NATO, while technology development is facilitated through ESA's optional ARTES programs with a budget of €8.4 million for 2018 (Euroconsult 2019).

### **Positioning, Navigation, and Timing (PNT)**

The Netherlands Positioning Service (NETPOS) is the GNSS reference network of the Land Registry and the Directorate of Infrastructure and Water Management. NETPOS makes it possible for surveyors with one GNSS receiver to determine their



position in the terrain within a few seconds and within a few centimeters. Companies that work for Ministry of Infrastructure and Water Management or the Land Registry may also make use of this. NETPOS has several GNSS reference stations spread over the Netherlands, with an average distance of 40 kilometers. This provides good coverage for the whole of the Netherlands. The data from the GNSS reference stations are used for obtaining geo-information, navigation, weather forecasts, education, and scientific research. NETPOS uses navigation satellites from both GPS (American) and GLONASS (Russian). In the future, the European Galileo will be added to this (NETPOS Website).

Funded by the Ministry of Infrastructure and Water Management, the IKUS Project (*Inventarisatie Kwetsbaarheden Uitval Satellietnavigatie*) addresses the issue of GNSS dependency and backup PNT solutions (Dutch Ministry of Justice and Security 2015). In August 2017, the Dutch Government released the report describing the resilience of critical GNSS infrastructure, focusing on the effects of space weather (Dutch Government 2017b).

The NLR undertook GPS and Galileo PRS interference field tests in 2017 (NLR 2017b). Further, the Netherlands participates to the optional ESA navigation programs in conjunction with the EU EGNOS/Galileo flagship program. In the frame of Galileo, the Galileo Reference Centre (GRC), the performance monitoring hub for the EU's global satellite navigation system, was officially opened in Noordwijk, in May 2018. The Centre will be operated by GSA with as main objective to ensure continuous Galileo accuracy below 20 cm. The GRC missions are as follows (GSA 2018): performing independent monitoring and assessment of Galileo service provision; assessing, when feasible, the compatibility and interoperability of Galileo vis-a-vis other GNSS; providing service performance expertise to the program; supporting investigations of service performance and service degradations; providing an archiving service for performance data over the nominal operational lifetime of the system; and integrating data and products from EU Member States and Norway and Switzerland.

### **Space Situational Awareness (SSA)**

The Ministry of Defense is, in collaboration with the TNO, NLR, and KNMI, researching space weather (Ministry of Justice and Security 2015). The Joint Meteorologische Group (JMG) located at the *Vliegbasis Woensdrecht* foresees the Armed Forces with space weather reports. The Netherlands' contribution to the optional SSA program at ESA amounted to €0.5 million in 2018 (Euroconsult 2019).

---

## **Norway**

### **Space and Security Budget**

Norway had an estimated defense expenditure of NOK 61.349 billion (€5.88 billion) or 1.8% of GDP in 2018, below the NATO guidelines of 2% of GDP (NATO 2019). In 2018, Norway's total space budget amounted to just above NOK 1 billion,

remaining stable compared with 2017. Norwegian investments for civil space activities have been steadily increasing in the past years, growing from NOK 569 million in 2014 to NOK 958 million in 2018. Defense space expenditure is estimated at NOK 80 million annually in the period 2016–2018 (for military satellite communications). The 2018 ESA contributions covered NOK 644 million. Although Norway gives preference to ESA programs over the national civil program, which represented 18% of the total civil expenditures in 2018, both budgets have increased in the past 5 years. The contribution to EUMETSAT for 2018 amounted to NOK 142 million (Euroconsult 2019). Norway is not a member of the EU but does work closely with the EU and its member states, as part of the European Economic Area (EEA) and the European Free Trade Association (EFTA).

## **Space and Security Activities and Programs**

### **Earth Observation (EO) – Intelligence-Surveillance-Reconnaissance (ISR)**

Norway relies on imagery procured from commercial providers, such as Inmarsat, Iridium, and Eutelsat, and international partners to support its tasks (Satellite Today 2015). The Norwegian CryoClim project is developing services for monitoring the cryosphere, i.e., the sea ice, snow cover, and glaciers in Norway and Svalbard. CryoClim will combine data from several different optical, meteorological, and radar satellites, including Radarsat-1 and Radarsat-2 (Norwegian Space Center 2018).

The NOFO (Norwegian Clean Seas Association for Operating Companies) and KSAT (Kongsberg Satellite Services) have signed an extended agreement for satellite-based remote sensing, on the Norwegian Continental Shelf, for detection of acute pollution from petroleum activity. This agreement represents a solid boost for the detection of oil spills on the Norwegian shelf, enabling rapid deployment of an oil recovery operation by having all fields in production monitored daily by satellite. KSAT has delivered its satellite-based oil spill detection service to the industry, through NOFO, since 2005 through KSAT ground stations (KSAT 2016).

Moreover, Norway is part of the Copernicus program in the frame of the EU and ESA. Norway participates in ESA's optional Earth observation programs, with a budget of €10 million for 2018 (Euroconsult 2019). Further, Norway is a member of the following international organizations: ECMWF, GEOSS, CEOS, and the WMO.

### **Satellite Communications (SATCOM)**

The Norwegian Space Centre's focus on infrastructure development has been of vital importance to the High North. The agency owns 50 percent of KSAT, with Kongsberg Defence & Aerospace owning the other 50 percent. KSAT operates satellite stations in Svalbard, Tromsø, and Antarctica. Due to the unique location of its polar ground stations, KSAT can provide maritime monitoring services and data from several radar and optical sources, delivered straight to the end user. The company also owns the fiber-optic cable linking Harstad on the Norwegian mainland to Longyearbyen, Svalbard. The Norwegian Space Centre has also leased capacity

from Telenor for broadband communications to Antarctica via the Thor 7 satellite (Norwegian Ministry of Industry and Trade 2012).

The Norwegian government announced in March 2018 the investment of NOK 1 billion for a new Arctic communications project implemented by Space Norway AS. The project is based on a system of two satellites providing coverage 24 h a day in the area north of 65 degrees N latitude. The expected life span of the satellites is 15 years and the satellites are expected to be launched in 2022. Space Norway AS owns the fiber-optic cable between Svalbard and mainland Norway, a key element of Norway's electronic infrastructure in the Arctic. Since 2015, the company has been working to establish satellite-based broadband communications capacity in the region (Barents Observer 2018).

Thales in Norway has supplied military and enterprise networks since the mid-1980s and has gained a broad experience in defense communications over the years. Thales has been selected by the Norwegian Armed Forces as the supplier for satellite communication systems for both the Nansen-class frigates and the Skjold-class corvettes. Additionally, Thales has been selected as sole supplier to NATO for securing IP networks with high-grade encryption for all classifications, including Cosmic Top Secret (CTS) (Thales Website).

Further, Norway is a member of the US-led WGS program and, also, a member of the IMO Global Maritime Distress and Safety System. Additionally, sharing of national SATCOM assets is facilitated through NATO, while technology development is facilitated through ESA's optional ARTES programs with a budget of €71 million for 2018 (Euroconsult 2019).

### **Positioning, Navigation, and Timing (PNT)**

The Norwegian satellites AISSat-1 and AISSat-2 monitor maritime traffic in Norwegian and international waters by detecting AIS (Automatic Identification Signals) from ships to determine their position, speed, and direction. The satellite project was realized as a collaboration between three Norwegian governmental institutions: the Norwegian Space Centre, the Norwegian Coastal Administration (NCA), FFI, Kongsberg Seatex, and KSAT. The satellite platform itself was purchased from Canada. The first AIS CubeSat was launched on the 12th of July 2010 from India to a polar orbit. AISSat-1 was primarily intended to demonstrate space-based AIS. Building on the experience and success with AISSat-1, a second identical satellite AISSat-2 was launched from Kazakhstan in July 2014. The third satellite in the AIS series, AISSat-3 was lost due to a launch failure from Russia in November 2017. The collaborating institutions use the data from AISSat-1 and AISSat-2 for a variety of purposes, including monitoring fisheries, oil spills, and maritime traffic, to support anti-piracy operations along the coast of Africa and other areas of interest to Norway (Norwegian Space Center Website).

Additionally, the Norwegian satellites NorSat-1 and NorSat-2 were launched in July 2017. The satellites including the satellite-AIS payloads are owned and commissioned by the Norwegian Space Centre, which will also be responsible for the operation of the two microsattellites. The receivers were developed by Kongsberg Seatex of Norway, with support provided by ESA through the SAT-AIS element of

ESA's ARTES program. The two satellites monitor maritime traffic and test science and technology payloads. In the Norwegian government's High North Strategy, further development of space-related infrastructure is a stated target. The satellite-based ship AIS is an important part of the integrated monitoring and notification system for the northern sea areas. The satellites are primarily financed by the Norwegian Coastal Administration and the Norwegian Space Centre (Norwegian Space Center Website).

In January 2018, the Norwegian Space Centre procured the final development NorSat-3 from Space Flight Laboratory in Canada. Combining a navigation radar detector and AIS receiver aims to enhance maritime awareness for the Norwegian Coastal Administration, Armed Forces, and other maritime authorities. The satellite is funded by the Norwegian Coastal Administration and managed by the Norwegian Space Centre. The Norwegian Defence Research Establishment is leading the development of the radar detector payload, which is funded by the Ministry of Defense. NorSat-3 is designed to capture signals from frequencies that the International Maritime Organization has allocated for civil navigational radars (Nordic Space 2018).

In August 2017, NASA signed an agreement with the Norwegian Mapping Authority to develop a Satellite Laser Ranging Station 1046 km from the North Pole that will produce high-precision locations of orbiting satellites, help track changes in the ice sheets, and improve the efficiency of marine transportation and agriculture. The Arctic station will be the latest addition to a global network of space geodetic stations. Under the partnership, the station will be built and installed in Ny-Ålesund, Svalbard. NASA will also provide expert consultation on how to operate the instruments. The Norwegian Mapping Authority started construction work on the new scientific base in 2014. The goal is to have all systems in operation by 2022 (NASA 2017).

Additionally, Norway is part of the COSPAS-SARSAT international satellite system for search and rescue. Further, Norway participates in the optional ESA navigation programs in conjunction with the EU EGNOS/Galileo flagship program.

### **Space Situational Awareness (SSA)**

The Norwegian Armed Forces Globus II radar at Vardø is used for space debris monitoring. The Globus II is a large X-band dish radar located at Vardo in Northern Norway. It is a dedicated sensor in the SSN and is used for tracking deep space objects, including objects in geosynchronous orbits, and for wide-band imaging of space objects. Originally known as HAVE STARE (AN/FPS-129), the radar became operational in 1995 at Vandenberg Air Force base in California. While there, it observed several intercontinental ballistic missile (ICBM) flight tests as well as two non-intercept tests of the kill vehicle for US national missile defense interceptor then under development (IFT-1A and IFT-2). Beginning in late 1998, HAVE STARE (AN/FPS-129) was dismantled and moved to Vardo, and then renamed Globus II. A previous radar named Globus was operational since the 1960s by Norway at Vardo, in cooperation with the US Air Force, used to monitor Soviet and Russian ballistic missile flight tests (Mostlymissiledefense 2012).

In 2013, the Birkeland Centre for Space Science was established as a Centre of Excellence in research. Its mission has been to increase knowledge of electrical current flows around the Earth, particle showers from space, auroras, gamma-ray bursts, and other links between the Earth and space (Norwegian Ministry of Industry and Trade 2012).

In April 2017, USSTRATCOM entered into an agreement with the Norwegian Ministry of Defense and Norwegian Ministry of Trade, Industry and Fisheries to share SSA services and information. The arrangement will enhance awareness within the space domain and increase the safety of spaceflight operations (US Strategic Command 2017). Norwegian SSA operations are also conducted within the ESA framework, with activities performed by the NMA and TGO. Norway's contribution to the optional SSA program at ESA was €1 million in 2018 (Euroconsult 2019).

---

## Sweden

### Space and Security Budget

In line with the Swedish Defence Policy 2016–2020, an increased defense budget is fundamental, particularly considering the deteriorating security situation, but also to address the need to increase warfighting capabilities of the Swedish Armed Forces. To that extent, the political agreement means that this defense bill adds approximately SEK 10 billion extra to the Armed Forces for the period of 2016–2020. Total defense spending in the period 2016 to 2020 amounts to SEK 224 billion for the Armed Forces, including defense intelligence (Swedish Government 2015).

In August 2017, the Swedish government reached an agreement on additional measures to increase the operational capabilities of military units and ensure overall total defense capability. In addition to the investments of SEK 500 million announced in the 2017 Spring Amending Budget, military capabilities and total defense capability will be enhanced with an additional SEK 2.7 billion per year from 2018. Top priority will be given to measures ensuring the implementation of the 2015 Defence Resolution during the period until the end of 2020. Priority will also be given to measures aimed at further enhancing capabilities during the current period and ensuring that military capabilities and total defense capability can increase after 2020. In accordance with the defense agreement, the allocated an additional SEK 80 million in 2018 to the National Defence Radio Establishment and the Military Intelligence and Security Service for efforts targeting counterterrorism, information and cyber security, and security services (Swedish Government 2017).

Swedish government expenditure on space amounted to SEK 1.1 billion in 2018, distributed between ESA programs (64%), national activities (21%), and EUMETSAT (15%). The 2018 ESA contributions covered SEK 696.8 million. The contribution to EUMETSAT for 2018 amounted to SEK 164 million (Euroconsult 2019).

## Space and Security Activities and Programs

### **Earth Observation (EO) – Intelligence-Surveillance-Reconnaissance (ISR)**

The Swedish National Space Agency (SNSA – Rymdstyrelsen) ran a National Earth observation program (Technopolis 2012). During the period 2001–2012, the program provided public funding amounting to SEK 219 million, of which SEK 133 million were related to projects in the research part and SEK 86 million to projects in the user's part. Until 2005, the two parts were of roughly equal size, but in recent years, the research part has come to significantly dominate the user's part. The beneficiaries in the research part have been dominated by a few universities and a government agency (Technopolis 2012).

Sweden participates in the French Pléiades program. Sweden is part of the Copernicus program in the frame of the EU and ESA. Sweden's contribution in ESA's optional Earth observation programs amounted €12.9 million for 2018 (Euroconsult 2019). Further, the Netherlands is a member of the following international organizations: ECMWF, GEOSS, CEOS, and the WMO.

### **Satellite Communications (SATCOM)**

Sharing of national SATCOM assets is facilitated through EDA and NATO, while technology development is facilitated through ESA's optional ARTES programs with a budget of €71 million for 2018 (Euroconsult 2019). Further, Sweden is a member of the US-led WGS program and, also, a member of the IMO Global Maritime Distress and Safety System. Additionally, sharing of national SATCOM assets is facilitated through NATO, while technology development is facilitated through ESA's optional ARTES programs with a budget of €6.18 million for 2018 (Euroconsult 2019). Sweden is also a member of the IMO Global Maritime Distress and Safety System.

### **Positioning, Navigation and Timing (PNT)**

A GNSS analysis center project has been started within the Nordic Geodetic Commission, chaired by Lantmäteriet (the Swedish mapping, cadastral, and land registration authority). The EGNOS Ranging and Integrity Monitoring Station that was inaugurated at Lantmäteriet in Gävle has been successfully supported by Lantmäteriet since 2003. SWEPOS is the Swedish national network of permanent GNSS stations and is operated from the headquarters of Lantmäteriet in Gävle (Lantmäteriet 2015).

SWEPOS provides real-time services on both meter level and centimeter level, as well as data processing. The SWEPOS Network RTK Service reached national coverage during 2010. Since data from permanent GNSS stations are exchanged between the Nordic countries, good coverage of the service in border areas and along the coasts has been obtained by the inclusion of 20 Norwegian SATREF stations, 4 Norwegian Leica SmartNet stations, 5 Finnish Geotrim stations, 1 Finnish Leica SmartNet station, 3 Danish Leica SmartNet stations, and 2 Danish Geodatastyrelsen (Danish Geodata Agency) stations (Lantmäteriet 2015).

Sweden is part of the COSPAS-SARSAT international satellite system for search and rescue. Further, Sweden participates in the optional ESA navigation programs in conjunction with the EU EGNOS/Galileo flagship program.

### **Space Situational Awareness (SSA)**

The Onsala Space Observatory (OSO), the Swedish National Infrastructure for Radio Astronomy, provides scientists with equipment to study the Earth and the rest of the Universe. OSO takes part in international radio astronomical projects. The observatory is a geodetic fundamental station. The equipment for Earth sciences includes navigation satellite receivers, a superconducting gravimeter, tide gauges, and radiometers (Chalmers Website).

The Swedish Institute of Space Physics (IRF) is a governmental research institute. Its primary task is to carry out basic research, education, and associated observatory activities in space physics, space technology, and atmospheric physics. IRF has employees in Kiruna, Umeå, Uppsala, and Lund. The research programs portfolio includes Solar Terrestrial and Atmospheric Research (STAR), Solar System Physics and Space Technology, and Space Plasma Physics (IRF Website).

Norwegian SSA operations are also conducted within the ESA framework, with activities performed by the NMA and TGO. Norway's contribution in the optional SSA program at ESA was €0.213 million in 2018 (Euroconsult 2019).

---

## **Switzerland**

### **Space and Security Budget**

Switzerland's defense spending is estimated to reach USD 6.5 billion in 2023, registering a compound annual growth rate (CAGR) of 4.67% between 2019 and 2023, according to a report by Strategic Defence Intelligence (SDI). Swiss defense budget spending in 2018 reported an increase of 6.7% in comparison with 2017, driven by the country's need to invest in new technologically advanced military equipment and devices to replace outdated equipment. Allocation of capital expenditure is anticipated to increase to an average of 24.7% of the total defense budget over the forecast period, compared with the average of 22.7% recorded during 2014–2018. Over the forecast period, Switzerland is expected to invest in command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR), and cybersecurity. The country intends to acquire unmanned aerial vehicles, critical infrastructure protection, and military radar, as well as upgrading its existing communications network and incorporating enhanced levels of Internet security (Army Technology 2018).

The 2018 space budget covered CHF 200 million, with CHF 166 million contribution to ESA and CHF 24 million to EUMETSAT (Euroconsult 2019). The Euroconsult identified budget does not include military space budget.

## Space and Security Activities and Programs

Although Switzerland invests most of its direct space funding through ESA, Switzerland has a so-called Programme for National Complementary Activities for Space (*Measures de Positionnement*), to encourage the emergence of space technology projects. It aims to develop niche sectors and to better position Swiss industrial and academic entities, particularly in the frame of ESA activities and other international programs such as the EU Research Framework Programmes. The Swiss Space Office (SSO) mandated the Swiss Space Centre (SSC) to implement the call for proposals 2018 (SSO 2018).

### **Earth Observation (EO) – Intelligence-Surveillance-Reconnaissance (ISR)**

In Switzerland, Earth observation data are being used in many fields, such as weather prediction, climate monitoring (e.g., clouds, air pollution, glaciers), landslide detection, or topographic mapping (SCNAT 2008).

Switzerland has no dedicated Earth observation satellite program. Switzerland's technology development at national level, it takes place namely at the Earth observation and Remote Sensing Group of the ETH Zurich Institute of Environmental Engineering (ETH Zurich Website). As an example of the use of space-based data for food security, the overall aim of the project Remote sensing-based Information and Insurance for Crops in Emerging economies ("RIICE") is to reduce the vulnerability of rice small-holder farmers in low-income countries in Asia and beyond. RIICE is implemented through a public-private partnership between the Deutsche Gesellschaft für Internationale Zusammenarbeit, the Swiss Agency for Development and Cooperation, the International Rice Research Institute, sarmap, and SwissRe (RIICE Website).

The objective of the Swiss Data Cube (SDC) is to support the Swiss government for environmental monitoring and reporting and enable Swiss scientific institutions (e.g., Universities), to facilitate new insights and research using the SDC, and to improve the knowledge on the Swiss environment using EO data. UN Environment/GRID-Geneva and the University of Geneva are currently building the Swiss Data Cube (SDC). Following the work done by Geoscience Australia the "Data Cube" is a new way for organizing Earth observations data. UN Environment/GRID-Geneva and the University of Geneva have developed a strong and fruitful collaboration around the SDC with the Committee on Earth Observations Satellites (CEOS), the Group on Earth Observations (GEO), and Geoscience Australia (Swiss Data Cube Website). The concept of the Data Cube is a series of structures and tools that calibrate and standardize datasets, enabling the application of time series and the rapid development of quantitative information products. The Data Cube approach calibrates this information to make it more accessible, easier to analyze and reduces the overall cost for users (Swiss Data Cube Website).

Moreover, Switzerland is part of the Copernicus program in the frame of the EU and ESA. Switzerland participates in ESA's optional Earth observation programs with a budget of €805.6 million for 2018 (Euroconsult 2019). Further, Switzerland is a member of the following international organizations: ECMWF, GEOSS, CEOS, and the WMO.



### **Satellite Communications (SATCOM)**

Switzerland has no dedicated SATCOM program. Switzerland has technology development at national level, for instance, at EPFL. The State Secretariat for Education, Research, and Innovation (SERI) cooperated with DLR on the development of satellite-based laser communications (DLR 2008).

RUAG and Elbit Systems (Israel) announced in November 2018 the signature of a Memorandum of Understanding to form a Joint Venture Company. The JVC will enable the companies to create synergies and leverage their respective competences and serve as a national Communication and System Competence Centre of Excellence. The Competence Centre will cater to the needs and requirements of the Swiss Federal Department of Defence, Civil Protection and Sport (DDPS). The Centre will act as a knowledge center to support the companies' joint efforts regarding a DDPS communication program of the Swiss Ministry of Defense and other joint endeavors in the future (Israel Defense 2018).

In September 2018, RUAG and SWISSto12 signed a partnership agreement committed to supply future satellites missions, including constellations of telecommunication satellites with crucial antenna solutions. The collaboration will focus on the development, design, and manufacturing of phased array antenna products that leverage the unique and complimentary offerings of both companies. SWISSto12, with their patented 3D printing technology, will provide innovative antenna system designs along with a manufacturing solution to 3D print the antenna in one highly integrated part combining, RF, mechanical and thermal functions. This approach aims at a high performance – at minimal cost and lead time for manufacturing and integration (RUAG 2018).

Further, Switzerland is a member of the IMO Global Maritime Distress and Safety System. Additionally, technology development is facilitated through ESA's optional ARTES programs with a budget of €9.5 million for 2018 (Euroconsult 2019).

### **Positioning, Navigation, and Timing (PNT)**

Swisstopo, the Swiss Federal Office of Topography, is responsible for the development, operation, and maintenance of a fundamental station and permanent stations of Switzerland's automated global navigation satellite systems. Swisstopo contributes, as one of several European processing centers of the European Permanent Network EPN. The Automated GNSS Network of Switzerland (AGNES) is a multipurpose reference network for national first order surveying, scientific research such as geodynamics, and GNSS meteorology and serves as a base for the Swiss positioning service (swipos). Swisstopo maintains the swipos positioning service for real-time applications. Switzerland is integrated into the international (IGS) and European (EPN) permanent networks via its Zimmerwald station. In the framework of the International GPS Service (IGS), the Federal Office of Topography set up a permanent GPS station in Zimmerwald in 1992. The data of this station are used by the Centre for Orbit Determination in Europe (CODE) at the Astronomical Institute of the University of Bern for the determination of highly precise GPS satellite orbits. The IGS provides the data from Zimmerwald geostation to interested parties for scientific research (Swisstopo Website).

The Swiss Federal Office of Civil Aviation, Zurich Airport, Geneva Airport, Switzerland's regional airports, SWISS, EasyJet, the Swiss Air Force, and skyguide have jointly established an innovation program called "CHIPS" for introducing new satellite-based flight procedures (Skyguide Website).

Further, Switzerland participates in the optional ESA navigation programs in conjunction with the EU EGNOS/Galileo flagship program.

### **Space Situational Awareness (SSA)**

The Zimmerwald Laser and Astrometric Telescope (ZIMLAT) has been designed for both satellite laser ranging and optical tracking with charge-coupled device (CCD) cameras, the latter mainly for orbit determination of space debris by means of astrometric positions. For the first time, a titanium-sapphire laser was introduced into a satellite laser ranging (SLR) tracking system. On 20th July 2009, Zimmerwald was the first European station which successfully sent laser pulses to the Lunar Reconnaissance Orbiter (LRO). In March 2012, the Graz and Zimmerwald SLR stations successfully conducted the first ever so-called "bistatic" laser ranging to a noncooperative target; the Zimmerwald SLR station for the very first time successfully detected and time – tagged photons sent by a powerful laser at the Graz SLR station and diffusely reflected by the body of the European ENVISAT spacecraft. In June 2013, photons reflected by a space debris object with a considerably smaller cross section than ENVISAT could be detected (Gutner and Ploner 2006).

The Swiss startup ClearSpace signed a debris-removal contract with ESA tasking the company with deorbiting a substantial piece of a Vega rocket left in orbit in 2013. For the pillar Space safety and security, Switzerland takes the lead in the removal of space debris thanks to ClearSpace, a spin-off from the EPFL Space Center focusing on developing technologies and services to remove unresponsive satellites from space. The startup has received funding for its ClearSpace-1 ADR mission under the ESA ADRIOS program. ESA has also selected ClearSpace to be the leader of the industrial consortium for the project (SpaceNews 2019).

Skyguide announced in March 2018 a partnership with AirMap to develop and deploy a national drone traffic management system for Switzerland. Swiss U-space, as it is known, will power Switzerland's thriving community of drone companies with UTM (Unmanned Traffic Management) services for advanced commercial drone operations like Beyond Visual Line of Sight (BVLOS) (Airmap 2018).

Switzerland's contribution in the optional ESA SSA programs was €1.12 million in 2018 (Euroconsult 2019).

---

## **Concluding Remarks**

This chapter provides evidence of the trend toward increasing relevance for security and defense in national space and security programs, together with the chapters on the largest and smaller European countries. "Space and security," both in its security from space and security in space aspects, are progressively contributing to further integration of space activities. Traditionally, only civilian space activities including,

for instance, Earth observation, telecommunications, human spaceflight, space transportation, and technology development were subject of cooperation projects at intergovernmental and supranational level. Security- or defense-related space programs were kept at the national level or dealt with bilaterally or multilaterally in *ad hoc* cooperative programs. These trends demonstrate an evolution of European countries priorities from strictly civil-oriented applications to also encompassing security and defense ones. National space programs with security or defense dimension, in combination with the EU and ESA programs, demonstrate alignment towards the use of space for security and defense. In this group of countries, the level of national space programs engagement varies, and often EU and ESA engagement is prime. To conclude, the increasing relevance of security and defense in Europe, to some extent, it could be framed as the necessity for Europe to take its security and defense into its own hands vis-à-vis other global space powers. Hence, this appears to be a stronger driver in the current geopolitical context.

**Disclaimer** The contents of this chapter and any contributions to the Handbook reflect personal opinions and do not necessarily reflect the opinion of the European Space Agency (ESA).

---

## References

- Airbus Defence & Space, Space Netherlands, OMI, Website. Available at: <http://www.airbusdefenceandspacenetherlands.nl/project/omi/>
- Airmap (2018) Swiss U-space powers life-saving drone pilot program in Switzerland, 6 June 2018
- Army-technology (2018) Report: Swiss defence budget to reach \$6.5bn by 2023, 4 May 2018
- Barents Observer (2018) Two new satellites to boost Norway's Arctic internet, 27 March 2018
- Belgian Ministry of Defence (2016) The Strategic vision for Defence, 29 June 2016, 29 June 2016
- Belgian Parliament (2017) Wetsontwerp Projet De Loi houdende de militaire programmering van investeringen voor de periode 2016- 2030, 7 November 2016, DOC 54 2137/001
- BELSPO Website. Belgian Federal Science Policy Office Earth Observation. Available at: [http://www.belspo.be/belspo/index\\_en.stm](http://www.belspo.be/belspo/index_en.stm)
- BEOP Website. Belgian Earth Observation, STEREO III. Available at: <https://eo.belspo.be/en/stereo-in-action>
- BMVIT (2017) Federal Ministry for Transport, Innovation, and Technology, Austrian Technology in Space – an overview of Austrian Space Industry and Research, August 2017
- Chalmers Website. Onsala Space Observatory. Available at: <https://www.chalmers.se/en/researchinfrastructure/oso/Pages/default.aspx>
- DLR (2008) Germany and Switzerland affirm their leading role in satellite communications, 28 November 2008
- Dutch Air Force (2017) Air force space command, wideband global SATCOM satellite, 22 March 2017
- Dutch Government (2017a) Nederlandse ruimtevaartinnovatie Tropomi gelanceerd, 13 October 2017
- Dutch Government (2017b) Rapport 'Inventarisatie Kwetsbaarheid Uitval Satellietnavigatie', 23 August 2017
- Dutch Ministry of Defense (2017) Materieelprojectenoverzicht – Prinsesjesdag 2017
- Dutch Ministry of Justice and Security (2015) Luchtmacht lanceert Space security center, Nationale Veiligheid en Crisisbeheersing, XIII-5, 2015
- ESA (2017) Pooling and sharing for government Satcoms, 21 November 2017

- ESA SSCC Website. SSA Space Weather Coordination Centre (SSCC). Available at: <http://swe.ssa.esa.int/web/guest/service-centre>
- ETH Zurich Website. Chair of Earth Observation and Remote Sensing – Current Projects. Available at: <https://eo.ifu.ethz.ch/>
- EUMETSAT (2018) Annual Report 2018. Available at: <https://www.eumetsat.int/website/home/AboutUs/Publications/AnnualReport/index.html>
- Euroconsult (2019) Government Space programs – benchmarks, Profiles & Forecasts to 2028, July 2019
- GPS World (2018) Galileo ground segment keeps constellation on track, 28 March 2018
- GSA (2018) Galileo reference Centre now officially open, 18 May 2018
- Gutner W, Ploner M (2006) CCD and SLR dual-use of the Zimmerwald tracking system, October 2006
- IRF Website. Swedish Institute of Space Physics (IRF), Research Programmes. Available at: <https://www.irf.se/en/>
- Israel Defense (2018) Elbit systems to form joint venture in Switzerland, 15 November 2018
- KSAT (2016) Kongsberg satellite services, increased use of satellite monitoring on the Norwegian Shelf, 5 October 2016
- Lantmäteriet (2015) The Swedish mapping, cadastral and land registration authority, Reports in Geodesy and Geographical Information Systems, Geodetic activities in Sweden 2010–2014
- MDA (2015) Case study NSO – developing the Netherlands geospatial community, May 2015
- Mostlymissiledefense (2012) Space Surveillance Sensors: Globus II Radar June 1, 2012
- NASA (2017) Norway to develop Arctic laser-Ranging Station, 07 August 2017
- NATO (2019) Defence expenditure of NATO countries (2013–2019) press release, PR/CP(2019) 123, November 2019
- Naval Technology (2009) Royal Netherlands Navy Chooses Thales-Built Satcom Solution, 12 October 2009
- NETPOS Website. Kadaster, The Netherlands Positioning Service NETPOS Available at: <https://www.kadaster.nl/netpos>
- NEWTEC (2018) Government and defense COTS SATCOM, March 2018
- NLR (2017a) Netherlands Aerospace Centre, Royal Netherlands Air Force and NLR strengthen partnership for information-driven air force operations, 8 December 2017
- NLR (2017b) Netherlands Aerospace Centre, GPS P(Y) vs Galileo PRS interference field test, presentation, 6 October 2017
- Nordic Space (2018) Developing of the Norwegian NorSat-3, 7 March 2018
- Norwegian Ministry of Industry and Trade (2012) Between heaven and earth: Norwegian Space policy for business and public benefit – Meld. St. 32 (2012–2013) Report to the Storting (White Paper)
- Norwegian Space Center Website, Norway's satellites. Available at: <https://www.romsenter.no/eng/Norway-in-Space/Norway-s-Satellites>
- NSO (2016) Space Policy – Policy Memorandum Space 2016 and NSO advisory report 2016
- NSO Website. Netherlands Space Office, National Programs. Sciamachy. Available at: <https://www.spaceoffice.nl/en/activities/national-programme/national-projects/sciamachy/>; Satellite Applications, Satellite Data Portal. Available at: <https://www.spaceoffice.nl/en/activities/satellite-applications/satellite-data-portal/>; Geodata for Agriculture and Water (G4AW). Available at: <https://g4aw.spaceoffice.nl/en/>
- Organization for Security and Cooperation in Europe – OSCE (2018) Republic of Austria, permanent Mission of Austria to the OSCE, exchange of information on the OSCE Code of conduct on politico-military aspects of security, 15 April 2015 and 16 April 2018
- Proba2 Science Centre Website, About the PROBA2 Science Center. Available at: <http://proba2.sidc.be/>
- RIICE Website. Remote sensing-based Information and Insurance for Crops in Emerging economies (“RIICE”), About RIICE. Available at: <http://www.riice.org/about-riice/about-riice/>

- ROB Website. Royal Observatory of Belgium, GNSS Research Group, GNSS Networks. Available at: [http://www.gps.oma.be/networks\\_tutorial.php](http://www.gps.oma.be/networks_tutorial.php)
- RUAG (2018) RUAG Space and SWISSto12 partner to supply advanced active antenna solutions for high throughput satellites, 14 September 2018
- Sagath D, Papadimitriou A, Adriaensen M, Giannopapa C (2018) Space strategy and governance of ESA small member states. *Acta Astronaut* 142:112–120
- Satellite Today (2015) Denmark Expects MilSatCom capacity Surge to continue, 9 April 2015
- SCNAT (2008) Significance of Earth Observation for Switzerland, Report of the Swiss Commission for Remote Sensing SCRS (Schweizerische Kommission für Fernerkundung SKF) Member of the Swiss Academy of Sciences SCNAT 2008
- Skyguide Website. Satellite-based navigation. Available at: <https://www.skyguide.ch/en/company/innovation/satellite-based-navigation/>
- Skywin (2015) Wallonie Espace Infos, no. 81, July–August 2015
- SpaceNews (2017) Luxembourg eyes earth-observation satellite for military and government, 7 November 2017
- SpaceNews (2019) Swiss startup ClearSpace wins ESA contract to deorbit Vega rocket debris, 9 December 2019
- SSO (2018) Swiss space office, call for proposals 2018 – to foster and promote Swiss scientific and technological competences related to space activities
- Swedish Government (2015) Sweden’s defence policy 2016 to 2020, 1 June 2015
- Swedish Government (2017) Budget 2018: increased military capabilities and enhanced total defence, 20 September 2017
- Swiss Data Cube Website. About Swiss Data Cube Website (SDC). Available at: <https://www.swissdatacube.org/>
- Swisstopo Website. Federal Office of Topography swisstopo, Permanent GNSS Networks. Available at: <https://www.swisstopo.admin.ch/en/knowledge-facts/surveying-geodesy/permanent-networks.html>
- Technopolis (2012) Technopolis Group, Faugert & Co Utvärdering AB, Impact evaluation of the Swedish National Space Board’s National Earth Observation Programme
- Thales Website. Thales Group, Europe, Security in Norway. Available at: <https://www.thalesgroup.com/en/countries/europe/norway/security-norway>
- TU Graz Website. Institute of Communication Networks and satellite Communications – Research Priorities. Available at: <https://www.tugraz.at/en/institutes/iks/home/>; TU Graz Q/V-Band, TUG, Q/V-band Optimised Transmission system. Available at: <https://www.tugraz.at/en/institutes/iks/nachrichtentechnik/aktuelle-projekte/qv-band-optimized-transmission-system/>
- UN-SPIDER (2014) Austria: earth observation data Centre for water resources monitoring, 7 October 2014
- US Strategic Command (2017) Belgium signs agreement to share space services data, 7 February 2017
- VITO Website. Flemish Institute for Technological Research (VITO), Remote Sensing technology; Product Distribution Portal; VITO, EO data made easily accessible. Available at: <https://www.vito-eodata.be/PDF/portal/Application.html#Home>



# Space and Security Programs in Smaller European Countries

# 64

Ntorina Antoni, Christina Giannopapa, and Maarten Adriaensen

## Contents

Introduction .....	1291
Czech Republic .....	1292
Space and Security Budget .....	1292
Space and Security Program .....	1292
Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR) .....	1292
Satellite Communications (SATCOM) .....	1293
Positioning, Navigation, and Timing (PNT) .....	1293
Space Situational Awareness (SSA) .....	1294
Denmark .....	1294
Space and Security Budget .....	1294
Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR) .....	1295
Satellite Communications (SATCOM) .....	1296
Positioning, Navigation, and Timing (PNT) .....	1297
Space Situational Awareness (SSA) .....	1297
Estonia .....	1298
Space and Security Budget .....	1298
Space and Security Program .....	1298
Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR) .....	1298
Satellite Communications (SATCOM) .....	1299
Positioning, Navigation, and Timing (PNT) .....	1300
Space Situational Awareness (SSA) .....	1300

---

N. Antoni (✉)

Eindhoven University of Technology, Eindhoven, The Netherlands

e-mail: [ntorina.antoni@gmail.com](mailto:ntorina.antoni@gmail.com)

C. Giannopapa · M. Adriaensen

European Space Agency (ESA), Paris, France

e-mail: [christina.giannopapa@esa.int](mailto:christina.giannopapa@esa.int); [maarten.cm.adriaensen@gmail.com](mailto:maarten.cm.adriaensen@gmail.com)

© Springer Nature Switzerland AG 2020

K.-U. Schrogl (ed.), *Handbook of Space Security*,

[https://doi.org/10.1007/978-3-030-23210-8\\_149](https://doi.org/10.1007/978-3-030-23210-8_149)

1289

Finland .....	1301
Space and Security Budget .....	1301
Space and Security Program .....	1301
Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR) .....	1302
Satellite Communications (SATCOM) .....	1303
Positioning, Navigation, and Timing (PNT) .....	1304
Space Situational Awareness (SSA) .....	1304
Greece .....	1305
Space and Security Budget .....	1305
Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR) .....	1305
Satellite Communications (SATCOM) .....	1306
Positioning, Navigation, and Timing (PNT) .....	1306
Space Situational Awareness (SSA) .....	1306
Hungary .....	1307
Space and Security Budget .....	1307
Space and Security Program .....	1307
Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR) .....	1307
Satellite Communications (SATCOM) .....	1308
Positioning, Navigation, and Timing (PNT) .....	1308
Space Situational Awareness (SSA) .....	1308
Ireland .....	1309
Space and Security Budget .....	1309
Space and Security Program .....	1309
Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR) .....	1309
Satellite Communications (SATCOM) .....	1310
Positioning, Navigation, and Timing (PNT) .....	1310
Space Situational Awareness (SSA) .....	1311
Luxembourg .....	1311
Space and Security Budget .....	1311
Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR) .....	1311
Satellite Communications (SATCOM) .....	1312
Positioning, Navigation, and Timing (PNT) .....	1313
Space Situational Awareness (SSA) .....	1313
Poland .....	1313
Space and Security Budget .....	1313
Space and Security Program .....	1314
Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR) .....	1314
Satellite Communications (SATCOM) .....	1315
Positioning, Navigation, and Timing (PNT) .....	1316
Space Situational Awareness (SSA) .....	1316
Portugal .....	1317
Space and Security Budget .....	1317
Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR) .....	1318
Satellite Communications (SATCOM) .....	1319
Positioning, Navigation, and Timing (PNT) .....	1320
Space Situational Awareness (SSA) .....	1320
Romania .....	1321
Space and Security Budget .....	1321
Space and Security Program .....	1321
Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR) .....	1322
Satellite Communications (SATCOM) .....	1323
Positioning, Navigation, and Timing (PNT) .....	1324
Space Situational Awareness (SSA) .....	1324
Concluding Remarks .....	1324
References .....	1325

---

**Abstract**

This chapter presents space and security programs of smaller European countries and indicates their main priorities and trends. In particular, it addresses space activities and programs in the fields of Earth observation (EO), Intelligence-Surveillance-Reconnaissance (ISR), Satellite Communication (SATCOM), Positioning, Navigation, and Timing (PNT), and Space Situational Awareness (SSA). The countries presented are Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Ireland, Luxemburg, Poland, Portugal, and Romania.

---

**Introduction**

The increased need for security in Europe and for Europe's space activities has led to several activities and programs developed in aerospace and defense. The main actors in Europe engaging in space and security activities are the European countries, the European Union (EU), and the European Space Agency (ESA). ► [Chap. 61, "Institutional Space Security Programs in Europe"](#) in this handbook describes how security and defense policies are progressively and gradually being supported by space programs of the EU and ESA, while the North Atlantic Treaty Organization (NATO) is also gradually involved. Space security policies of the various European countries are to a large extent determined by national needs and priorities, as explained in ► [Chap. 25, "Space and Security Policy in Selected European Countries."](#) In addition, the policies are influenced by the overall space and security governance and their participation in relevant organizations as explained in ► [Chap. 23, "Strategic Overview of European Space and Security Governance."](#)

Hence, various space security activities and programs are to a large extent determined by national needs and priorities as well as participation to space and security relevant organizations, including the EU and ESA. The current chapter addresses space and security budgets, activities, and programs of selected European countries in the fields of Earth observation (EO), Intelligence-Surveillance-Reconnaissance (ISR), Satellite Communication (SATCOM), Positioning, Navigation, and Timing (PNT), and Space Situational Awareness (SSA). European countries may be distinguished not only based on their membership to space and security related organizations but also based on their space budget. In the absence of an official grouping of these countries, their ESA annual budget and their defense expenditure as a share of their growth domestic product (GDP) are used in this chapter, to classify them into three groups (Sagath et al. 2018).

The group presented in this chapter includes ESA member states with a GDP up to €350 billion and an annual ESA space budget (2018 ESA budget) typically up to €35 million: Czech Republic, Denmark, Estonia, Finland, Greece, Hungary, Ireland, Luxemburg, Poland, Portugal, and Romania (Sagath et al. 2018). This chapter complements the chapters on the largest and medium-sized European countries presented in this handbook. The content is up to date until January 2019.



## Czech Republic

### Space and Security Budget

In 2018, the country's defense budget was valued at CZK 59.75 billion (€2.35 billion) or 1.19% of GDP in 2018, below the NATO guideline of 2% of GDP. The national defense budget for 2018 was 10.8% higher compared with 2017 (NATO 2019). The Czech government expenditure for space-related activities amounted to €53.06 million in 2018, resulting from parallel contributions to ESA (€857 million) that doubled compared to 2014 (Euroconsult 2019). The space budget is expected to rise more in the future (Czech Ministry of Transport 2014). No military space budget has been identified by Euroconsult.

### Space and Security Program

Czech Republic's space activities include (Ministry of Transport 2016): contributions to the ESA mandatory and optional programs and to the EUMETSAT program; space applications development activities in several sectors, e.g., transport, industry and environment, and resource management; and space-related scientific research at universities and institutes of the Czech Academy of Sciences.

The 2003 launched MIMOSA (Microaccelerometric Measurements of Satellite Accelerations) was a microsatellite of the Czech Republic, designed and developed at the Astronomical Institute/Academy of Sciences (ASU/CAS) of Ondřejov. The project was funded by the Grant Agency of the Czech Republic. The overall mission objective was to obtain total density distributions in space and time of the upper ionosphere by sensitive measurements of the nongravitational orbital perturbations including atmospheric drag and solar radiation pressure (EO Portal Website). Furthermore, VZLUSat-1, a 2 U CubeSat Czech technology nanosatellite of VZLU, developed in cooperation with Czech companies (RITE, HVP Plasma, 5 M, TTS, IST) and universities (CVUT, University of West Bohemia). VZLUSat-1 is still operational (EO Portal Website).

### Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR)

The Czech priorities in Earth observation include development of new geoinformatics products from EO data; application of SAR data for monitoring of infrastructure statics, multispectral, and hyperspectral data for environment applications, land use, land cover, monitoring, natural disasters etc.; cooperation in development of services for downstream GMES/Copernicus market; development of integrated applications using EO data; and development of high-tech optical systems including active and adaptive optics (Czech Ministry of Transport 2016).

The Czech Republic has in place bilateral cooperation with France. In November 2018, the French Space Agency – CNES President underlined the success of bilateral space cooperation between France and the Czech Republic, exemplified by the Taranis mission. The mission aims to study storm phenomena in the atmosphere and plans to launch in 2019. Charles University in Prague has been working closely with France’s LPC2E and IRAP research laboratories to deliver the data processing unit and the instrument for detection of energetic electrons for this program. Similarly, Charles University’s space physics laboratory is working with IRAP to develop an instrument for Europe’s Solar Orbiter mission, which is set to launch in 2020 (CNES 2018).

The Czech Republic is participating to the Copernicus program in the frame of the EU and ESA. The Czech contribution to ESA Earth observation programs amounted to €2.23 million in 2018 (Euroconsult 2019).

### **Satellite Communications (SATCOM)**

The Czech Republic contributes to satellite communication activities through ESA’s optional ARTES programs, with a budget of €6.91 million for 2018 (Euroconsult 2019).

The Czech priorities in SATCOM include design of communication terminals; design and manufacture of satellite platform mechanisms; analysis of application of electromagnetic waves propagation models; and development and manufacturing of control and monitoring systems for ground segment (Czech Ministry of Transport 2016).

### **Positioning, Navigation, and Timing (PNT)**

The Czech Republic participates in the optional navigation programs in conjunction with the EU EGNOS/Galileo flagship program. The European GNSS Agency (GSA) seat is in Prague.

The Czech priorities in PNT include monitoring and educational tools for EGNOS/Galileo; design of GNSS receivers and other sensors; GNSS signal processing; Smart GNSS antennas; GNSS only and integrated applications combining EO satnav, satcom, and other technology/data; and analysis of GNSS reliability and security (Czech Ministry of Transport 2016).

The Czech Republic has four complementing GNSS permanent networks: CZEPOS, commercial network of permanent GNSS stations in the Czech Republic operated by the COSMC; GEONAS, geodynamic GNSS network in the Czech Republic operated by the Institute of Rock Structure and Mechanics of the Czech Academy of Sciences; PPGNET, network of permanent GNSS Stations in Greece operated by the Research Institute of Geodesy, Topography, and Cartography, Geodetic Observatory Pecny, and the Charles University in Prague, Faculty of Mathematics and Physics, Department of Geophysics in close cooperation with the

Seismological Laboratory of University of Patras; and VESOG, research and experimental network of permanent GNSS stations in the Czech Republic operated by the Research Institute of Geodesy, Topography, and Cartography, Geodetic Observatory Pecny (Czech GEO Data Portal Website).

The Geodynamic Network of the Academy of Sciences (GEONAS) of the Czech Republic was established in order to make regular geophysical and geodetic observations for current geodynamic studies of the Bohemian Massif and adjacent Central European geological structures. The permanent GNSS stations have been set up, since 2001, by the Institute of Rock Structure and Mechanics, Acad. Sci. (IRSM) within the framework of the national center of Earth Dynamics Research activities. All stations register both NAVSTAR and GLONASS satellite signals. Some of these stations are located inside the regional geodynamic networks for epoch GPS measurements (Schenk et al. 2010).

## Space Situational Awareness (SSA)

The Czech Republic contribution to the optional SSA program at ESA amounted to €455 thousand in 2018 (Euroconsult 2019).

The Czech priorities in SSA include (Ministry of Transport 2016): tracking of near-Earth objects; studies, modeling, and monitoring (photometry, follow-up) of asteroids (including NEOs), together with characterization of rotational periods, surfaces of small meteoroidal bodies, and their interactions with the Earth's atmosphere; follow-up astrometry of newly discovered NEOs, recoveries of NEOs, and comets; control and tracking systems for telescopes and ground station antennae; large volume data processing, computing capacities; European Fireball Network (using mostly optical instruments but also including specialized radio antenna for monitoring of daytime meteors) – many stations located in the Czech Republic and abroad; and Ionospheric, Radiation and Interplanetary Space Weather dealing with space plasma physics aimed at the ionosphere and magnetosphere of the Earth (ionospheres and magnetospheres of planets of the solar system) and at the study of solar wind.

The potential use of the high-tech laser center (ELI Beams) in Dolni Brezany has been considered in the frame of A2/AD satellite dazzling and asteroid defense (ESJ News 2018).

---

## Denmark

### Space and Security Budget

In 2018, Denmark recorded GDP growth of 1.2%, one of the highest GDPs per capita in Europe (Euroconsult 2019). Denmark had an estimated defense expenditure of DKK 28.78 billion (€3.85 billion) or 1.32% of GDP in 2018, below the NATO guideline of 2% of GDP. 18.1% of the 2018 estimated budget was allocated to

equipment expenditure (NATO 2019). The new Defence Agreement for 2018–2023 represents a substantial investment. It aims to increase defense spending with DKK 800 million in 2018 and an increased trend to DKK 4.8 billion more expenditure in 2023. This is an increase in defense spending by more than 20 per cent as well as a significant increase in equipment investment (Danish Ministry of Defence 2017). Denmark does not have a national space budget. Instead it funds its space activities via ESA and the European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT). In 2018 its contribution to ESA was €30.6 million and to EUMETSAT €7.7 million. The space defense budget in the field of telecommunications was €8 million in 2018 (Euroconsult 2019).

### **Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR)**

The Danish armed forces use Earth observation satellite imagery to provide reconnaissance in support of: detecting oil spills, and enforcing sanctions on environmental polluters, ice breaking and monitoring, and sea search and rescue operations (Danish Ministry of Defence 2016).

The Danish policy paper “Strategy for the Arctic 2011–2020” underlines that security and sovereignty in the arctic space is exercised through the presence of the Danish armed forces. To bolster the reconnaissance capability, this presence provides the Danish Defence Acquisition and Logistics Organization signed in 2016 a public-private partnership with DTU Space and satellite company GomSpace to develop a test surveillance nanosatellite dubbed “Ulloriaq” (means star in Greenlandic) and “GOMX-4A.” Launched in February 2018 from the Jiuquan Satellite Launch Center in China (together with GOMX-4B), the project is used to evaluate the usefulness and cost-effectiveness of nanosatellites for monitoring naval vessels and aircraft in the arctic, and for assisting with its search and rescue responsibilities. When the project ends in 2020, it will be clearer whether this type of space equipment can contribute to the task performance of the Danish armed forces. The armed forces are to evaluate the usefulness of such a satellite system in relation to the possibility of obtaining a better “situational picture” of the Arctic region in the future. The idea is that the satellite will contribute to the monitoring of the Danish Ministry of Defence’s area of responsibility in the Arctic and form part of the civilian tasks performed by the armed forces in the area including sea rescue (DTU 2018).

GOMX-4 are twin siblings following the successful GOMX-3 mission and represent the new generation of nanosatellite platforms. GOMX-4B is funded by ESA, and it has been designed to be the most advanced CubeSat for IOD. It is based on the innovative and flexible 6 U platform from GomSpace, and it shall demonstrate the operations of six payloads on board. The main payloads are 6 U propulsion modules from NanoSpace, the innovative S-band Inter-Satellite Link (ISL) from GomSpace and the High-Speed Link from GomSpace with high data rate capacities. Additionally, this satellite accommodates the Radiation Hardness Assurance Board,

called Chimera, developed by ESA to evaluate the behavior in space of different ceramic memories and two new optical devices, the HyperScout hyperspectral camera from Cosine and a star tracker developed by ISIS. Even with different payloads and mission goals, the two satellites will work together using an Inter-Satellite Link to optimize their capabilities to share data and to transmit it to ground. The life expectancy of the GOMX-4 nanosatellites is 3–5 years, and they are expected to be fully operated by GomSpace during that period (DTU 2018).

GomSpace is a Danish-Swedish nanosatellite manufacturer. The company's business operations are mainly conducted through the wholly-owned Danish subsidiary, GomSpace A/S, with operational office in Aalborg, Denmark (Satnews 2017). Beyond GOMX-4A, Denmark possesses no independent Earth observation capabilities. It has to rely on imagery procured from commercial providers, such as Inmarsat, Iridium, and Eutelsat, and international partners to support its tasks (SatelliteToday 2015). Nonetheless, in addition to the arctic strategy, the country's "Defence Agreement 2018-2023," "Space Strategy 2016," and "Agreement on the future missions of the Danish Ministry of Defence," all recognize that heightened economic and military activity in arctic space will necessitate the increased presence of the Danish armed forces in the region and consequently further investments in EO capabilities. As such, there is a likelihood that helicopter and drone-based surveillance will gradually be replaced with high-resolution satellite imagery (DTU 2018).

Denmark operates three unarmed maritime patrol aircraft over the Baltic Sea and off Greenland. The 2012 Defence Agreement includes substantial funds for testing different additional surveillance options for the Arctic, including UAVs and the use of existing satellites (SIPRI 2016).

In addition to ESA, EUMETSAT, and the EU, Danish public authorities also take part in other international cooperation collaborations. Through the Arctic Council, Danish authorities are involved in various projects concerning infrastructure in space and the use of satellite data. The Ministry of Defence works together with Canada on the exchange of surveillance data (Danish Government 2016). Denmark's position for sharing and pooling of EO is mainly centered around the bilateral approach, implemented in cooperation agreements with direct partners (mainly Scandinavian Countries, Canada, France, and the US in addition to others).

Denmark is participating to the Copernicus program in the frame of the EU and ESA. Denmark's contribution to ESA's optional Earth observation programs amounted to €4.2 million for 2018 (Euroconsult 2019).

## **Satellite Communications (SATCOM)**

Sharing of national satcom assets is facilitated through NATO, while technology development is facilitated through ESA. Denmark took part in satellite communication activities through ESA's optional ARTES Programs, with a budget of €1.19 million for 2018 (Euroconsult 2019).

The Danish company DataPath Inc. was awarded a €6.5 million contract in 2015 to provide five Wideband Global Satcom (WGS) terminals with related equipment

and training for the Danish Air Force and 29 Wideband Global Satcom (WGS) terminals with related equipment and training for the Danish Army (SIGNAL 2015).

Moreover, the Wideband Global Satcom-9 (WGS), part of the US-led WGS system is funded jointly by Canada, Denmark, Luxembourg, the Netherlands, and New Zealand. The system was launched in March 2018. The contribution gives the countries access to the US-controlled WGS military communications system (ViaSatellite 2016). In this regard in May of 2016, the SES S.A. announced that it will provide two anchor stations for the Danish Defence Acquisition and Logistics Organization (DALO). Under the agreement, SES Techcom Services, a wholly-owned subsidiary of SES, will provide and maintain two WGS system anchor stations – one in X-band and one in Ka-band. This will enable the Danish armed forces to communicate through the system, which provides flexible, high-capacity communications for defense operations through the associated satellite constellation and control systems. SES was awarded the contracts based on its experience in providing satellite communication anchor stations, the associated WGS certification process and overall life-cycle cost criteria. The Danish forces will join other nations partnering with the US in the WGS program and thus offer the US State Department satellite-based communication services to users, including marines, soldiers, sailors, airmen, and the White House Communications Agency (SES 2016).

### **Positioning, Navigation, and Timing (PNT)**

The Danish Ministry of Defence has access to the civil and military signals of the US GPS system. GPS is evolving, with the introduction of GPS III satellites and the modernization of the ground segment.

The Division for Geodesy at DTU Space researches the maintenance and development of geodetic infrastructure and development of new techniques for surveying and mapping. Research in the field of geodetic infrastructure is carried out as a basis for spatial infrastructure, including surveying and mapping. Research in the field of positioning is being carried out with the aim of developing new techniques for surveying and navigation purposes. Furthermore, it also makes it possible to monitor the integrity of satellite systems and detect problems. A major effort is also being put into the detection of ice load changes in Greenland based on permanent GPS combined with campaign measurements (DTU Space Website).

Denmark participates in the optional navigation programs in conjunction with the EU EGNOS/Galileo flagship program.

### **Space Situational Awareness (SSA)**

Activities related to the Earth's electromagnetic environment are carried out in Denmark mainly at DMI and DTU Space. DTU Space has been involved in space weather research FP7 Coronal Mass Ejections and Solar Energetic Particles (COMESPEP). Additionally, SSA activities are pursued within the ESA framework. Moreover, The Danish Ministry of Defence and US Strategic Command

(USSTRATCOM) signed a data sharing agreement in April 2018 to share space situational awareness (SSA) services and information (SpaceNews 2018). Further, Denmark contributes to the optional SSA program at ESA, with the amount of €0.24 million in 2018 (Euroconsult 2019).

---

## **Estonia**

### **Space and Security Budget**

Estonia's 2018 defense budget remains one of the most balanced in Europe. According to the NATO defense budget methodology, which differs somewhat from the national methodology, personnel expenditures account for 30%, procurement and investments 27%, and other costs 43% of defense expenditures. An additional €15 million is added to Estonia's 2018 defense budget from the NATO Security Investment Program (NSIP), the majority of which is intended for the training of the NATO Very High Readiness Joint Task Force (VJTF) at the central training area and the hosting of units during a period of crisis. Therefore, a total of more than €586 million, representing 2.11% of the forecast GDP, is available for spending within the area of government of the Ministry of Defence. It is divided in 21% of defense expenditures in 2019, with infrastructure investments and procurement costs accounting for 43% and all other spending 36% (NATO 2019, Estonian Ministry of Defence 2019). The Estonian government expenditures for space-related activities amounted to €6.7 million in 2018, which has doubled compared to 2014 (Euroconsult 2019). No military space budget has been identified by Euroconsult.

### **Space and Security Program**

Estonia sent its first nanosatellite ESTCube-1 into space (€100 thousand cost) in May 2013 after 6 years of development by over a hundred students and scientists. The aim of ESTCube-1 was to popularize science and engineering among students. It served as the basis for 48 research projects, 5 doctoral theses and has generated 6 spin-off companies to date. The first satellite is followed by ESTCube-2 and TTU100 projects. In 2014, Tallinn University of Technology (TUT) established the Mektory Space Centre, where more than 15 academic supervisors and 40 students from various disciplines are involved in the nanosatellite program (Investinestonia 2017).

### **Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR)**

The Estonian Land Board is responsible for the national mirror site (ESTHub) for providing free access to Sentinel satellite data. ESTHub will collect and archive datasets that cover the Estonian territory and a buffer zone of about 200 km. These

datasets will be freely available and downloadable for anyone, but the required notices on the data source must be provided (Estonian Land Board Website).

The Mektory Space Centre is working on the TTÜ100 satellite project. The main mission of the TTÜ100 satellite is Earth observation and demonstration of Earth observation technologies. The satellite includes cameras, image processing, and communication with ground station. The cameras include the RGB sensor for visual light image and the NIR sensor for near-infrared image that can be used for assessing vegetation growth, climate, geology, and sea conditions (TTU Website).

The Estonian Marine Institute Department of Remote Sensing and Marine Optics mainly focuses on developing optically complex remote sensing methods, suitable for coastal sea and inland waters, and applying those methods. The department also studies the relationship between underwater light field and wildlife. Specific research fields are, for example, identifying the flowering of potential toxic phytoplankton and its quantitative sensing with remote sensing methods, mapping of phytobenthos, and the depth of shallow waters using satellites and sensors, which are located on the planes, and researching the global carbon cycle. Furthermore, the department concentrates on developing primary production models and remote sensing methods for evaluating the quality of the water in Baltic Sea and in lakes (Estonian Marine Institute Website).

Additionally, Estonia is involved in the HYPERNETS Project. The HYPERNETS project is coordinated by the Royal Belgian Institute of Natural Sciences. Besides Estonia, there are project partners from six countries: France, Argentina, Italy, Germany, and the UK. In the project which includes Tartu Observatory as a partner, an instrument for the support measurements of optical remote sensing satellites is created. The support measurement instruments will form a worldwide remote sensing network with unified data processing and management (University of Tartu 2018).

Technology development is facilitated through ESA. Estonia participates in the Copernicus program in the frame of the EU and ESA. Estonia's contribution to ESA Earth observation programs covered a budget of €590 thousand in 2018 (Euroconsult 2019).

## **Satellite Communications (SATCOM)**

Estonia is also a member of EDA. Estonia joined the EDA EU Satcom Market in January 2017. The EDA EU Satcom Market since its start in 2012 under the name EU SatCom Procurement Cell (ESCP). The EDA EU Satcom Market today comprises 28 contributing members including Estonia (EDA Website). In addition, Estonia participates in the EDA Project Team on Satellite Communications and is part of the Ad Hoc Working Group preparing the establishment of the EDA GOVSATCOM Demonstration Project (pooling and sharing). Further, technology development is also facilitated via NATO. Estonia is a member of NATO since 2004. Estonia's primary defense capability forms a military force that supports the activation of NATO's collective defense mechanism. Estonia does not develop all its



military capabilities independently, instead as a NATO member, the Estonian Defence Forces can develop capabilities in cooperation with NATO allies (Estonian Ministry of Defence).

### **Positioning, Navigation, and Timing (PNT)**

ESTPOS is the Estonian GNSS-RTK permanent stations network consisting of continuously operating reference stations. The first GNSS (Global Navigation Satellite System) CORS (Continuously Operating Reference Station) in Estonia became operational in 1996 in Suurupi, established by ELB in cooperation with the Finnish Geodetic Institute (FGI). Starting from 2008, four Estonian CORS are incorporated into the EPN (EUREF Permanent GNSS Network). A few years later more Estonian GNSS CORS were established. In 2008 new CORS were set up in Kärda (KARD), Mustvee (MVEE), and Võru (VOR2, initially denoted VORU) and outdated equipment in MUS2 was replaced. Currently the total number of the resulting ESTPOS reference stations is 28. These ESTPOS stations were interconnected to the national geodetic network by a special GNSS campaign in 2017. Modernized ESTPOS is an important part of Estonian geodetic reference system (Metsar et al. 2018).

The Ministry of Defence makes use of the US Global Positioning System (GPS), which provides position, velocity, and time information to an unlimited number of users, through civilian and encrypted military modes. The Ministry of Defence relies on the GPS system until the full operational capacity of Galileo (including PRS). The dependency on GPS is a logical consequence of NATO membership and the fact that GPS is the only globally available GNSS network. In the future, in all EU and NATO framed operations, military GNSS receivers will simultaneously use Galileo and GPS, increasing accuracy and resilience (Muls 2016).

Estonia cooperated with Switzerland on the construction of a GNSS-RTK permanent station network ESTPOS from May 2014 until September 2015. In addition, cooperation with Finland and Latvia is envisaged (Estonian Land Board 2015).

### **Space Situational Awareness (SSA)**

In the context of SSA, the event-timing devices being developed by Eventech are regarded of good quality and have a promising market both for SSA and in-orbit applications. According to a recent study, on Latvia's participation in the European Space Agency since 2015, the event timers could potentially be considered for developing further the SSA program but also under the GSTP programs of ESA (Invent Baltics OÜ 2019). The Institute of Astronomy of the University of Latvia operates the station RIGL 1884, part of the International Laser Ranging Service105 managed by NASA. This expertise, along with the leading Latvian technology in event-timing devices, could be further explored (Invent Baltics OÜ 2019).

## Finland

### Space and Security Budget

Finland had an estimated defense expenditure of €2.8 million or 1.23% of GDP in 2017. 19.9% of total defense budget goes to procurement of materiel and 10.8% on real estate expenditure. Finland's Ministry of Defence proposed a €3.2 billion defense budget for 2019, a €326 million, or 11%, increase from 2018. The ministry said on 9 August 2018, that this would increase the country's defense budget's share of GDP from 1.23% in 2018 to 1.32% in 2019. The Ministry of Defence attributed much of the increase –€260 million – to spending on the Laivue (Squadron) 2020 program in order to build a new class of four multipurpose offshore patrol vessels. Nearly €1.2 billion, or 43.6%, of the budget will be allocated to equipment readiness. Defense procurement contracts account for €771 million (Finnish Ministry of Defence 2018).

During 2013–2020, Finland set to invest €400 million in ESA's and European Commission's space programs. Finland's contribution to the ESA budget in 2018 was €20 million (0.6%) which is less than half of the share corresponding to the Finnish GDP (1.40%). The Finnish public sector funding to space activities is €50 million including the payments to ESA and EUMETSAT. The Ministry of Economic Affairs and Employment proposed budget authorizations for the grants of Business Finland, the Finnish Funding Agency for Innovation, of slightly more than €344 million, which is almost €74 million more than in the approved 2018 budget figure. Slightly more than €102 million is proposed as Business Finland's operating costs, which is an increase of more than €18 million compared with the Budget for 2018. The space budget identified by Euroconsult does not include space-related military expenses (Finnish Ministry of Economic Affairs 2018; Euroconsult 2019).

### Space and Security Program

The main space activities in Finland include space science, Earth observation, satellite positioning and satellite telecommunications, and the satellite equipment industry. Each area has basic research, applied research, and business and applications exploiting space technology for the needs of the citizens, for the public sector, and for commercial purposes. The foundation of Finnish space activities is the participation to European organizations. ESA's programs are the backbone of the Finnish space activities, which are also influenced by Finland's membership in EUMETSAT, ESO and European Commission's space activities such as Galileo, Copernicus, and the space activities in Horizon 2020 (Finnish Ministry of Economic Affairs and Employment 2013).

There are about 90 operators in Finland that are engaged in the development of space technology applications. There are dozens of satellite navigation companies in Finland including: u-Blox (positioning electronic circuits), HERE (maps), Reaktor (small satellites), Iceye (small satellites), Mobisoft, Aplicom and Paetronics (vehicle

management), Beaconsim (simulators), Alpha, Positron, and SSF (pseudolites, which can replace satellite signals in such places as container ports and open-cast mines), Suunto and Sports Tracking Technologies (sports), Tracker (tracking of hunting dogs), and Vaisala (measurement equipment and systems). The combined turnover of the Finnish companies producing satellite navigation systems and equipment is at least €300 million (Finnish Ministry of Transport and Communications 2018). Additionally, Business Finland's New Space Economy program offers funding, networks, and export services for developing international space-related business. The New Space Economy program funds startup companies that are reforming the sector, growth-seeking manufacturing companies, and businesses focused on data utilization. The ESA Business Incubation Centre Finland supports this objective (Business Finland Website).

On 18 April 2017, Aalto-2 became the first Finnish-built satellite to be launched into space from Cape Canaveral, Florida. Then on June 23, Finland's Aalto-1 carried the world's smallest hyperspectral imager into space on the Polar Satellite Launch Vehicle sent up by the Indian Space Research Organization. The Aalto-1 and Aalto-2 missions have ignited the rise of astrophysics and the establishment of a NewSpace sector in Finland. Independent space companies, the first space law, and a Finnish space program are set to reshape traditional technologies, develop faster and cheaper access to space than ever before, and advance earth observations far beyond today's satellite capabilities. The first satellite, Aalto-1, had two initial goals: (1) a technology demonstration of the state-of-the-art payload and (2) serve as a learning curve in the operation and management of space missions for future launches (Science Business 2017).

## **Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR)**

The Finnish startup ICEYE plans an 18-satellite constellation of SAR (synthetic-aperture radar) equipped microsatellites. The ICEYE imaging radar instrument can image through clouds, obscuring weather, and darkness. In 2017, ICEYE secured USD 2.8 million in R&D funding from SME Instrument within EU Horizon 2020 as well as USD 2.8 million financing from private entities. Additional funding was received from the Finnish Funding Agency for Innovations. ICEYE-X1 is ICEYE's first proof-of-concept microsatellite mission with a SAR sensor as its payload. It was launched on January 12, 2018, on ISRO's PSLV-C40 rocket from Satish Dhawan Space Center in India. ICEYE-X1 is also the world's first SAR satellite in this size (under 100 kg), enabling radar imaging of the Earth through clouds and even in total darkness. The satellite is the very first Finnish commercial satellite. Following the January 2018 launch of ICEYE-X1, ICEYE, the two newest SAR satellites were launched in July 2019 (ICEYE 2019, ICEYE Website).

Additionally, the Finnish Meteorological Institute (FMI) Earth Observation Research unit focuses on remote sensing of the atmospheric composition and the cryosphere as well as the development of retrieval methods. The cryospheric

processes group investigates the use of Earth observation data in understanding the water and carbon cycles in the Arctic, northern tundra, and boreal forest regions. The group has been involved in research projects funded by the European Space Agency focusing on Polar regions and cryosphere products (FMI Website). In April 2018, Finland and China signed an agreement to establish a joint research center for Arctic space observation and data sharing services. The China CAS and Finnish FMI will jointly build a research center in Sodankyla, north Finland's Lapland. The center will enhance cooperation on cryosphere research with satellites, which will provide information from the Arctic region for use in climate research, environmental monitoring, and operational activities, such as navigation in the Arctic Ocean. The two countries agreed to build the center as a platform for international cooperation in research on the Arctic region, and a model of Sino-European space-based Earth observation application cooperation. In 2016, China Remote Sensing Satellite North Polar Ground Station (CNP GS) was built in Sweden. The agreement is the latest move of China's Digital Belt and Road Program, which was initiated in 2016 to improve environmental monitoring and promote data sharing (CAS 2018).

During the last India-Nordic Summit in April 2018, the Finnish Prime Minister highlighted the opportunities for cooperation between our two countries that exist especially in sectors such as energy, satellites, and education. Finland and India have agreed to deepen cooperation in these fields and will hold further negotiations on concrete projects (Finnish Government 2018). In addition, in the frame of the Finnish Presidency of the Arctic Council and the meteorological cooperation program, FMI considers themes that would include monitoring of the Arctic, especially the increased utilization of satellite data in operational activities and services; supporting research that aims to increase an understanding of the Arctic environment; and launching of new service concepts to support Arctic functions and increase safety in the Arctic. Moreover, in July 2017, the Finnish and Italian Ministries of Defence signed a framework agreement on cooperation regarding the COSMO-SkyMed Second Generation radar imaging satellite system (Finnish Ministry of Defence 2017).

Finland participates in the Copernicus program in the frame of the EU and ESA. Finland's contribution to ESA Earth observation programs covered a budget of €5.1 million in 2018 (Euroconsult 2019).

## **Satellite Communications (SATCOM)**

Norsat International Inc. has provided satellite communication equipment and services for the Finnish Defence Forces since in 2009. Following the success of the network used during an European peacekeeping mission in Chad, the armed forces requested that Norsat assist them in expanding their communication network to support an ongoing mission in Afghanistan. In this field, Norsat's rugged, portable satellite terminals consistently provide communication links in the extreme environmental conditions of desert deployments, wet conditions, and cold Northern winters (Norsat 2012).

Moreover, the Finnish 5GKIRI project aims to support the construction of 5G networks through more agile and nationwide processes. The participating cities are

Espoo, Helsinki, Jyväskylä, Kuopio, Lahti, Oulu, Turku, and Vantaa, and the project is being coordinated by Sitowise Oy. Commercial operations on 5G networks can begin at the start of 2019 (FICORA 2018).

Further, Finland's contribution to satellite communication activities through ESA's optional ARTES programs amounted to €1.4 million for 2018 (Euroconsult 2019).

## **Positioning, Navigation, and Timing (PNT)**

Finland's objectives and priorities regarding PNT and GNSS relate to the specific geographic position of the country. Satellite navigation programs and their associated support systems do not perform optimally at high latitudes and especially in the Arctic region in particular in determining vertical positioning. This is due to the satellite constellation, i.e., the way satellites are situated on their orbits. However, Galileo provides a somewhat better coverage in higher latitudes than GPS, whereas GLONASS provides the best possible coverage due to its highest inclination angle. There are problems with geostationary navigation systems (EGNOS) in Northern Europe, because the satellites that send support signals are poorly visible in northern areas, and the good reception is not possible. Additionally, resilience against potential interference and jamming of signals is a priority (Ministry of Transport and Communications 2018).

The Ministry of Transport and Communications has set out a draft operational program on satellite navigation. The program describes the current state of satellite navigation systems and how they are deployed in different sectors, especially in automated transport. Finland aims to develop automated maritime transport in line with their maritime strategy and policy (Finnish Ministry of Transport and Communications 2018).

The National Land Survey of Finland (NLS) operates a nationwide GNSS network of 20 stations. The NLS Finnish Geospatial Research Institute performs research on Arctic navigation including ice-aware maritime route optimization using satellite imagery (VORIC, STORMWINDS, and ESABALT projects), enhanced situational awareness for maritime operation, and developing methods for autonomous driving in arctic conditions and contributing to Aurora Snowbox, a test area for autonomous driving in Northern Finland (NLS 2017).

Finland participates in the optional navigation programs in conjunction with the EU EGNOS/Galileo flagship program.

## **Space Situational Awareness (SSA)**

The Finnish institutes involved in space weather activities include universities (Helsinki, Oulu, Turku, and Aalto), research institutes (FMI, Finnish National Land Survey), and companies (e.g., Isaware, ASRO, KNL Networks, and RF Shamans). Finnish activities include projects in operational services and research, and missions for new measurement and space transportation technologies. Besides its national service, Finland is active partner also in the operational services by the

Space Situational Awareness (SSA) program of ESA. Finnish contributions are included in the Expert Service Centers on Space Radiation, Geomagnetic activity, and Ionospheric weather. Finland participates in the optional ESA SSA program with an amount of €324 thousand in 2018 (Euroconsult 2019).

---

## Greece

### Space and Security Budget

Greece had an estimated defense expenditure of €4.5 billion or 2.28% of GDP in 2018, well above the NATO guideline of 2% of GDP (NATO 2019). Greek government expenditure on space amounted to €19.8 million in 2018. Greece contributed 10.3 million to ESA and €7.5 million to EUMETSAT in 2018 (Euroconsult 2019). Greece announced in 2019 the increase in its contribution to the ESA optional programs from 8.5 million to 33 million for the next 3 years (Infocom.gr 2020). No military space budget has been identified by Euroconsult.

### Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR)

The National Observatory of Athens has an Institute for Astronomy, Astrophysics, Space Applications, and Remote Sensing working on a variety of nationally, EU and ESA funded projects, including Earth observation applications (National Observatory Website). Greece participates in collaborative programs at regional (i.e. Mediterranean, Southeast Europe), ESA, and EU level. There is a strong interest and potential of the Greek Earth Observation community toward downstream services and applications development including security aspects. In the context of ISR, the Greek Ministry of National Defence has recently expressed its intent to lease from Israel seven Heron medium-altitude, long-endurance (MALE) unmanned aerial vehicles (UAVs) for 3 years. The systems will be used to monitor refugee flows in the country (C4Defense 2018).

Since 2007 Greece has participated in the French Helios 2 program. In addition, Greece is a member of the French program Composante Spatiale Optique (CSO). Since 1999 the governments of Belgium, France, Germany, Greece, Italy, and Spain have been working on an agreement called the Common Operational Requirements for Global European Earth Observation System by Satellites – more commonly known by its French acronym BOC. The aim was to define common requirements for military or dual-use Earth observation systems in the visible infrared and radar domains (Schrogl et al. 2015).

Greece is participating to the Copernicus program in the frame of the EU and ESA. Greece participates in ESA's optional Earth observation programs. Additionally, in March 2019 Greece and ESA agreed on the development of a national program on Greek Earth Observation Microsatellites for 5 years (Mononews 2019).

## **Satellite Communications (SATCOM)**

Since 2019, Greece together with Luxembourg are the only countries, apart from the largest five countries in Europe, that they have their own operational governmental satellite communications system. The Greek system is referenced as GreeCom or KLEIDDI (key in Greek) operated by the Ministry of National Defence in cooperation with the General Secretariat of Telecommunications and Post of the Ministry of Digital Governance responsible for civilian space matters (TaNea 2019). The civilian part is installed in all high-level governmental offices, parliament, civil protection, police, and embassies outside Greece. It is based on the exploitation of Greek frequencies and orbital position of the Hellas Sat satellites. These are operated by Hellas Sat which is a satellite communications solutions provider offering coverage over Europe, Middle East, and Southern Africa. It has operated since 2001 upon licenses provided by Greece and Cyprus, and the Greek license was renewed in 2017 (Euractiv 2019). Hellas Sat 2 was launched in May 2003; Hellas Sat 3 was launched in June 2017; and Hellas Sat 4 was launched in February 2019. Further, Greece engages with the EU, EDA, and ESA ARTES in view of the European Governmental Satellite Communications (GOVSATCOM).

## **Positioning, Navigation, and Timing (PNT)**

Greece participates in the EGNOS Ground Segment, which comprises a network of Ranging Integrity Monitoring Stations (RIMS), two Mission Control Centers (MCC), and two Navigation Land Earth Stations (NLES) per GEO satellite. The main function of the RIMS is to collect measurements from GPS satellites and to transmit these raw data every second to the Central Processing Facilities (CPF) of each MCC. The initial configuration included 34 RIMS sites located over a wide geographical area. In order to improve the performance of the EGNOS system and enlarge the area where the EGNOS services can be used, additional RIMS were deployed in Athens, Greece, as well as in Spain and Egypt (ESA Navipedia).

## **Space Situational Awareness (SSA)**

The National Observatory of Athens has an Institute for Astronomy, Astrophysics, Space Applications and Remote Sensing working on a variety of national, EU and ESA funded projects, including space weather (National Observatory Website).

The Arichtarchos telescope has been used in the frame of near-Earth object (NEO) activities analyzing lunar impact. NELIOTA is an activity initiated by ESA, which was launched in February 2015 at the National Observatory of Athens and was running until November 2018. The project determined the frequency and distribution of NEOs by monitoring the non-illuminated side of the Moon for flashes caused by NEO impacts, which result in the formation of a crater on the surface of

the Moon. NELIOTA will help assess the threat of small NEO collisions to orbiting spacecraft and to future ESA Moon missions (National Observatory Website).

Greece participates in the ESA SSA program.

---

## Hungary

### Space and Security Budget

The 2018 defense budget of Hungary was valued at HUF 484 billion. The country had an estimated defense expenditure of 1.21% of GDP in 2018 below the NATO guideline of 2% of GDP (NATO 2019). Euroconsult estimates the Hungarian 2018 space budget at €10.5 million, with €6.2 million contribution to ESA and €3.5 million to EUMETSAT (Euroconsult 2019). No military space budget has been identified by Euroconsult.

### Space and Security Program

Masat-1, the first Hungarian satellite, captured the first satellite space photographs on March 8, 2012 over the southern section of the African continent. Masat-1 reentered the atmosphere in January 2015 (Innoteka 2018). The 3-year-long operations of MaSat-1, the Hungarian contribution to the Rosetta mission, and the accession to the European Space Agency have laid down the foundations for the future of Hungarian space activities (Hungarian Space Office – HSO 2016).

In June 2016, Hungary announced the work on two additional satellites, RadCube and Smog-1, to be launched in 2020. The new space laboratory established at the Hungarian Academy of Sciences Research Centre (MTA EK) is instrumental for the testing and validation of the new satellites (Innoteka 2018).

### Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR)

Within the Government Office of Budapest, the Earth Surveying and Remote Sensing and Land Office in the Cosmic Geodesy Department is the central surveying and mapping organization in Hungary. The activities of the Institute include the maintenance of national data bases, professional information systems, data processing, research and development in the fields of surveying, mapping, and remote sensing. The Department's Satellite Geodetic Observatory (SGO) is an internationally recognized center of satellite geodesy. It is active in basic research (geodynamics, meteorology), applications, development and services related to Global Navigation Satellite Systems (GNSS), as well as interferometric synthetic-aperture radar (InSAR) research and its applications (HSO Department of Geodesy).



A combined national multi-technique (SAR, GNSS, leveling) geodetic network was established with the support of ESA in 2015. They have been studying various scientific and practical applications of SAR data from the Sentinel-1 satellites of the EU-ESA Copernicus program. The Department is playing a key role in national and European land monitoring activities (HSO Department of Geodesy).

### **Satellite Communications (SATCOM)**

The BME Department of Broadband Infocommunications and Electromagnetic Theory has participated to the ESA Alphasat programme with a propagation and a communication experiment. It developed the power subsystem and Langmuir-probe experiment for the ESEO satellite. The coordination of the Masat-1 project, furthermore to the development of the satellite's onboard communications system, and the establishment and operation of the ground control station were major achievements of the Department. The Department also participates to the radar image processing of the Sentinel-1A satellite (HSO BME).

Hungary became a founding member of the Intersputnik International Organization of Space Communications in 1971. Intersputnik has 26 Member States. The organization serves the purpose of the co-development of space-based telecommunications capabilities.

Technology development in Hungary is facilitated through ESA.

### **Positioning, Navigation, and Timing (PNT)**

The current national permanent GNSS network "GNSSnet.hu" consists of 54 permanent stations: 35 in Hungary and 19 in adjacent countries through cross-border data exchange. The Cosmic Geodesy Observatory has created and maintains this GNSS network for GNSSnet.hu, capable of performing authentic geodetic tasks. The stations' data are continuously transmitted to the GNSS service provider in real time, where a central software balances the measurements together to produce the corrections necessary to make field measurements more accurate (GNSSnet.hu Website).

### **Space Situational Awareness (SSA)**

The research group at the Eötvös Loránd University, focuses on satellite remote sensing, research related to Earth's magnetosphere and involvement in international scientific projects. In the field of space physics, and in particular space weather research, the group focuses mainly on the theory of electromagnetic wave propagation in magnetized plasmas and its practical applications (HSO, Eötvös).

## **Ireland**

### **Space and Security Budget**

Defense spending increased in the 2019 Irish budget by €47.5 million to almost €1 billion, though most of the €994 million was absorbed by the pay bill. Capital spending jumped from €29 million to €106 million (Irish Examiner 2018a). Euroconsult estimates the Irish 2018 national space budget at €17.4 million ESA contribution and €6.5 million EUMETSAT contribution (Euroconsult 2019). No military space budget has been identified by Euroconsult.

### **Space and Security Program**

Ireland's first satellite, the EIRSAT-1 completed the Critical Design Review phase of the European Space Agency's program in September 2018. The successful completion of this first stage of the Fly Your Satellite (FYS) program is regarded as an important milestone in the project, with the satellite currently on track to be completed within the next 2 years. EIRSAT-1 is led by a team of students from UCD and funded by the Irish Research Council, Science Foundation Ireland and the European Space Agency. The CubeSat will be launched from the International Space Station, where it will join a multitude of other objects in Earth's orbit. As it stands the EIRSAT-1, team expect the satellite to be delivered to the ESA by mid-2020. After launch the satellite will operate for between 6 and 12 months in orbit, communicating data from space to the mission control in UCD (Irish Examiner 2018b).

The ESA Space Solutions Centre Ireland and its ESA Business Incubation Centres (BIC) are one of 16 ESA BICs developed to create viable businesses and new jobs (Tyndall Website).

### **Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR)**

Engagement with space-based EO has primarily been within specific interest areas, such as the work of Met Éireann with ESA and EUMETSAT and research links with the international satellite observations community. Ireland's strategic location on the western boundary of Europe and its relatively clean environment have been factors in attracting research interest and links to the international satellite analysis community. Long-term operational use of satellites has been confined to the area of meteorology, with only a limited appreciation of how they can be used in other areas. Consequently, focused investment in promoting education, research, development, and operational use of EO has not occurred, while there has been a major

investment in other sensor development areas and associated information and communications technology (ICT). This has resulted in inertia among the potential user communities, which prefer to rely on conventional methodologies and data streams for core activities, and a dearth of a significant well-trained and informed research community in this area (EPA 2011).

Moreover, the National Centre for Geocomputation (NCG) was established in 2004 at the Maynooth University. The center covers a diverse range of research areas including Earth observation; mobile mapping systems, including unmanned aircraft systems (UAS); geospatial modeling; spatial statistics; geovisualization; interoperability; and cloud-based architectures (Maynooth University 2014).

Additionally, Ireland is participating to the Copernicus program in the frame of the EU and ESA. Ireland participates in ESA Earth observation programs with a budget of €1.06 million in 2018 (Euroconsult 2019). Ireland signed a Technical Collaborative Agreement with ESA in October 2017 regarding the access to Copernicus data. This arrangement provides Ireland with unprecedented access to the Copernicus program's near-real-time Earth observation information. The data will be stored locally for research, commercial development and policy informing purposes (Irish Government 2017).

## **Satellite Communications (SATCOM)**

The US company Viasat announced in April 2018 the opening of its expanded Dublin office, with nearly 100 team members located in Dublin primarily developing innovative software solutions for the commercial aviation industry. Viasat expects to more than double its headcount in Dublin over the next few years and extend development beyond connected aircraft software to include broader software and mobile application support for international maritime customers, European residential broadband and Wi-Fi markets, government systems as well as support for Viasat's next-generation ultra-high capacity satellite platform known as ViaSat-3 (DBEI 2018).

Moreover, Ireland participates in satellite communication activities through ESA's optional ARTES programs, with a budget of €1.35 million in 2018.

## **Positioning, Navigation, and Timing (PNT)**

The active GNSS network for Ireland is the result of collaboration between Ordnance Survey Ireland (OSi) and the Ordnance Survey of Northern Ireland (OSNI). The Irish National Grid (ING) is realized through a continuously operating reference system (CORS) network of active GNSS systems consisting of the 17 OSi network stations and 6 OSNI Stations (FIG 2013).

Further, Ireland participates in the optional navigation programs in conjunction with the EU EGNOS/Galileo flagship program.

## Space Situational Awareness (SSA)

The Rosse Solar-Terrestrial Observatory ([RSTO](#)) at the Dublin Institute for Advanced Studies (DIAS) has three eCallisto solar radio burst monitors operating at 10–400 MHz, a 4-element LOFAR/LBA test array, ionospheric monitors, and a magnetometer operated by DIAS Geophysics ([DIAS Website](#)).

---

## Luxembourg

### Space and Security Budget

Luxembourg defense expenditure totaled €301 million or 0.56% of GDP in 2018, below the NATO guideline of 2% of GDP. 45.1% of the 2018 estimated budget was allocated to equipment expenditure (NATO [2019](#)). The Luxembourg total space expenditure amounted to €78 million in 2018 of which €49 million covered civil activities and €29 million defense. The amount has significantly increased from €53 million in 2017 (Euroconsult [2019](#)). Since Luxembourg's adhesion to ESA in 2005, its annual contribution has increased €3.3million to €26.6 million in 2018. Initially, Luxembourg's military space expenditure covered entirely its contribution to the US WGS military communication program, but later it increased due to the funding of the SES16/GovSat with investment by both SES and the government (Euroconsult [2019](#)). The Euroconsult numbers may not fully reflect the expenditure by Luxembourg on Govsat-1, the National Advanced Optical System (NAOS) and WGS.

### Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR)

After deciding on the establishment of a national GOVSATCOM system, the next priority for Luxembourg was the establishment of a national Earth observation system, in line with the ambitious defense strategy implementation by 2025. Luxembourg wanted governmental system (not military) with first goal to have national capacity for imagery and at the same time be provider for EU, NATO, and partner countries (role of image provider at governmental level (Security Luxembourg [2018](#))).

The National Advanced Optical System – NAOS – aims to be a single satellite system operating in LEO SSO Polar orbit, equipped with a panchromatic and hyperspectral camera payload. Two ground stations will provide data upload and download. Two TT&C stations in Luxembourg will be deployed. Luxembourg is making an approved client list (including EU, NATO, and other organizations and nations) and partners will be able to program tasks. Expected operational lifetime is 10 years (Paperjam [2018](#)). OHB Italia was responsible for the preliminary study completed in April 2018. The Luxembourgian Parliament approved the Government Proposal for NAOS and corresponding draft law (€170 million excluding VAT

in the military equipment fund until 2028) in July 2018, with 2 votes against out of 60 votes. The launch and start of operations are expected in 2022. The NAOS satellite will increase Luxembourg's military spending from 0.4% to 0.6% of GDP (Paperjam 2018).

Luxembourg is benefiting from Belgian expertise in the NAOS Programme. LUXGOVSAT will become the operator and the Belgian Ministry of Defence is supporting payload operations for LUXGOVSAT. Luxembourg will be the sole owner of the system, but Belgium will acquire programming rights in cooperation with Luxembourg (Belgian Ministry of Defence 2017).

Presented by the Ministry of Economy in April 2018, Luxembourg has invested through ESA (EOEP, InCuBed, IAP, Copernicus) and national programs (collaborative ground segment and high-power computing) €45 million in support of EO infrastructure and service development (Ministry of Economy 2018).

## Satellite Communications (SATCOM)

Luxembourg entered global space activities in 1985 through the creation of the Société Européenne des Satellites (SES), a landmark for satellite telecommunications and a major player in this sector. This initiative led to the development of an entire space industry in Luxembourg (The Luxembourg Government 2016). Luxembourg's involvement in satellite communications is built on the heritage and capabilities that revolve around SES, created in 1985, and builds on the legacy of ESA's ARTES program for technology R&D activities. The involvement of SES in European projects provides opportunities for the Luxembourg space industry. For example, LuxSpace (an OHB subsidiary) will provide a microsatellite platform to support the demonstration mission of the European space-based Automatic Dependent Surveillance Broadcast (ADS-B) air traffic control project (Euroconsult 2019).

Luxembourg's MilSatcom needs are covered by participation to WGS and NATO. Luxembourg's GOVSATCOM needs are now covered by the national GOVSAT system.

The 2015 procurement of GOVSAT-1 contributes to Luxembourg's strategy of becoming more involved with NATO (Euroconsult 2019). On 31 January 31 2018, Luxembourg launched the GovSat-1 communication satellite. GOVAT-1, which possesses reliable satellite communication capacity for military and civilian purposes, meets growing demand from institutions and the defense sector. While part of the capacity of the GOVAST-1 satellite will be used to meet the Grand Duchy's needs in terms of satellite communication using military frequencies, it is intended that its remaining communication capacity will be sold on to allied and partner countries and to international organizations (including NATO and the EU). The satellite is being operated by LUXGOVSAT SA, a public-private joint venture created in 2015 by the Luxembourg State and SES (Security Luxembourg 2018).

GovSat-1 is a multi-mission satellite that offers X-band and Military Ka-band capacity over Europe, Africa, the Middle East, and substantial maritime coverage over the Mediterranean and Baltic Seas, as well as over the Atlantic and Indian Oceans. GovSat-1 is a highly secure satellite with encrypted command and control, and anti-

jamming capabilities (SES 2018). The GOVSAT applications include Institutional Security Applications: Civil-military interagency collaboration, Strategic and tactical networks, Emergency response, Disaster recovery, Protection of natural resources, and Remote government offices; and Defense Applications: Remote army operations (Mission to HQ communications), Communications on the move (COTM), Communications on the pause (COTP), Maritime operations, and Aero operations (ISR) (GovSat 2018).

In November 2016, GovSat (brand under LUXGOVSAT SA) announced that it has been granted a long-term commercial SATCOM contract to support the operational phase of NATO Alliance Ground Surveillance (AGS). The contract for an end-to-end service includes the delivery of satellite capacity in commercial Ku-band as well as associated capacity management support to provide the required command and control as well as sensor data communications between the NATO Global Hawk UAVs and ground segment over the AGS operational area. GovSat will be ensuring the provision of the Satcom services out of its security cleared facilities with dedicated security cleared personnel, also deployed within NATO premises. With this agreement, Luxembourg Authorities and the NCI Agency as procurement executive agent respectively acquire and manage the services provided by GovSat (GovSat 2016). The Luxembourgian program also fits in the EU GOVSATCOM initiative (Space News 2017).

## **Positioning, Navigation, and Timing (PNT)**

In May 2018, SES signed a long-term agreement with Spaceopal. The contract is part of the Galileo Service Operator (GSOp) framework agreement between Spaceopal – a joint venture between Telespazio and DLR GfR mbH – and the GSA. Under the agreement, SES will provide Spaceopal with services to support the maintenance and seamless operations of the Galileo Global Navigation Satellite System (GNSS). SES will be responsible for in-orbit measurements for the Galileo satellite constellation and provide VSAT managed services to Telespazio for the Galileo Data Dissemination Network (GDDN) (SES 2018).

## **Space Situational Awareness (SSA)**

SSA is currently mainly pursued through cooperation in the frame of ESA.

---

## **Poland**

### **Space and Security Budget**

Poland had an estimated defense expenditure of PLN 42.824 billion or 2.00% of GDP in 2018, matching the NATO guideline of 2% of GDP (NATO 2019). The 2016 Euroconsult numbers do not account for any military spending on space in Poland. The Polish government expenditure for space-related activities amounted to PLN

339.5 million in 2018, distributed between contributions to ESA (43%), national activities (39%), and EUMETSAT (18%) (Euroconsult 2019).

## Space and Security Program

The National Space Program of Poland includes support for the development of satellite systems, technological development as well as integration and development of infrastructure for the purposes of data processing and sharing center, support for administration, education, and higher education (Science in Poland 2017). Under this program, the funds provided by the Ministry of Investment and Economic Development are to be allocated to support the development of an astronomical observation satellite, a SAR microsatellite, and a number of other R&D projects in Poland's space sector, among others (Space R&D 2018).

## Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR)

The SAT-AIS-PL project is implemented by a consortium of Polish scientific, research, and business organizations. The aim is to create a satellite-based automated maritime traffic identification system (SAT-AIS) for the defense and security of Poland. The project is implemented in close cooperation with ESA and the European Maritime Safety Agency (EMSA). The first Polish satellite built for the use in the SAT-AIS-PL system will be a part of a constellation of satellites of other EU countries with a view to increasing the efficiency of the automatic maritime traffic identification system by collaborating with those countries for the exchange of satellite data (Polish Government 2017).

With support from EU regional development funding, the National Institute of Meteorology and Water Management (IMGW) in consortium with the Space Research Centre of the Polish Academy of Sciences, the Academic Computer Centre CYFRONET AGH, and POLSA is conducting since the end of 2017 the project "Operating system for gathering, sharing and promotion of digital information about the environment" (Sat4Envi). The aim of the Sat4Envi project is to create infrastructure for receiving, storing, processing, and distributing data from Sentinel-1, Sentinel-2, Sentinel-3 satellites, and satellite products based on existing IMGW resources. Thanks to its implementation, data from, among others, Copernicus program missions available for Poland will be enabled to public administration to be applied in its activities related to environmental protection, area development and planning, development of urbanization, and transport networks, and to private entities to create commercial services. The project has received over PLN 17.9 million funding under the Operational Programme Digital Poland (Science in Poland 2018).

On June 8, 2017, the Polish subsidiary of Thales Alenia Space, Poland's state-run defense group PGZ, and Warsaw University of Technology publicly announced their intention to jointly found a concurrent design facility. The facility is to create a

satellite design center, also known under the name of Concurrent Design Facility under the responsibility of the Ministry of National Defence. It shows the country's effort to construct its first Earth observation satellite development of satellite technology by 2030 (Defence24 2017).

On December 18, 2017, two Polish companies, Creotech Instruments (SA) and Wrocław Institute of Spatial Information and Artificial Intelligence (WIZIPISI) signed an alliance with Planetek Italia. The cooperation aims to further increase research in the field of Earth observation along with the development and commercialization of joint solutions (Planetek Italia 2017).

To reach the objectives of the Polish Space Strategy and to meet the requirements of the Ministry of Defence, Poland is investing in optoelectronic satellites. The tender pertaining the creation of reconnaissance satellites was planned by 2017 with a program value estimated at 700 million PLN (Defence24 2016a). The first high-resolution satellite could be used both for military, as well as for civilian applications, a dual-use purpose system, delivering the information both for the Army, as well as for the national services. The very-high resolution satellite would be used solely for military purposes. The main goal of the whole program would be to create a national visual reconnaissance system while stimulating the Polish aerospace and space industry for technology development. In accordance with the 2017 Polish Space Strategy, the satellites should be launched and fully operational by 2024 (Defence24 2016b).

Experience gained during the work on the optoelectronic satellite will facilitate the construction of the radar reconnaissance satellite. Also, national know-how from the construction of ground-based radars will be used, with a view to completing the project by the end of 2025 (Polish Government 2017). The initial feasibility study on the SAR system was ordered by POLSA at the end of 2015. A consortium led by Airbus Defence and Space PZL "Warszawa-Okęcie" S.A. branch was the contractor. The Polish Army uses the COSMO-SkyMed Second Generation system in accordance with the agreement between the Polish Ministry of Defence and its Italian counterpart. The Polish Ministry of Defence is participating in the COSMO-SkyMed program with the role of "international defense partner" (Telespazio 2015). Moreover, a specialized satellite reconnaissance center is being created in Poland. The Polish Defence User Ground Segment station is going to be created, within the territory of Poland, in Białobrzegi, north of Warsaw with full capability expected in 2020 (Defence24 2016a).

Furthermore, Poland participates in the Copernicus program in the frame of the EU and ESA. Poland participates to ESA Earth observation programs with a budget of €3.72 million in 2018 (Euroconsult 2019).

## **Satellite Communications (SATCOM)**

Poland has begun the initial stage of the conceptual works related to a Polish telecommunications satellite which, above all, would be tasked with a defense-related mission. Acquisition of a satellite of this class would secure the needs of our country within the domain of obtaining independent transfer capabilities



pertaining to the military satellite data. System of this type would also facilitate communications between the military units, including the units deployed abroad. The above program is especially significant when one considers the NATO commitments made by Poland, along with the involvement of the Polish armed forces in foreign deployments (Defence24 2016b).

The recent experiences suggest that permanent access to a broadband data connection needs to be provided for the units of the Polish Military Contingent, to maintain communications with command. At the same time, it shall be expected that, as high quantity and volume of data is becoming more and more accessible, the demand for expanding the capabilities within that scope would also be an area of a continuous growth. Up until now, access to the telecommunications-transferred data for the Polish forces has been provided through provision of access to the US Army and NATO satellite assets, as well as through application of satellite connectivity assets provided by commercial entities (Defence24 2016b).

In the establishment of Polish satcom capabilities, it is agreed at national level that civil-military cooperation in the development of the Polish communication satellite system is needed. It is also important for Poland to participate in international space programs that will improve the qualifications of Polish scientists and to allocate more funds for research and development activities (Polish Institute of Aviation 2018).

Poland participates to satellite communication activities through ESA's optional ARTES programs, with a budget of €0.94 million for 2018 (Euroconsult 2019).

## **Positioning, Navigation, and Timing (PNT)**

The Armament Inspectorate of the Polish Ministry of Defence announced a tender in 2016 to acquire 1244 military-grade GPS units featuring the SAASM (Selective Availability Anti-Spoofing Module) system (Defence24 2016c). Also, Poland has requested to buy to the US eight universal position navigation units, 34 low-cost reduced-range practice rockets and 1,642 guidance and control section assemblies for GMLRS along with other test sets, devices, and GPS receivers (Defence News 2017).

The European GNSS Agency GSA-supported POSITION (Polish Support to Innovation and Technology IncubatiON) project has worked to increase E-GNSS market penetration and general awareness within the country. Specifically, the project focuses its efforts on startups and early stage investment opportunities for Polish companies looking to utilize E-GNSS technology (Inside GNSS 2017).

Further, Poland participates to the optional navigation programs in conjunction with the EU EGNOS/Galileo flagship program.

## **Space Situational Awareness (SSA)**

SSA is a priority for Poland, identified in the Polish Space Strategy. Before the adoption of the Strategy in 2017, Poland had been active in the development of its national SSA capabilities. Poland has an objective to establish an operations center

for the surveillance and tracking of space objects (Space Surveillance and Tracking – SST) enabling the acquisition and processing of information about the current and predicted situation in space (Polish Government 2017).

In July 2015, the National Centre for Research and Development had announced a competition, the aim of which is to create an automated system for optical monitoring and tracking, under the name of SST PL. SST PL was considered a necessary condition and stepping stone to join the EU SST Consortium. Within the framework of the SST-PL project realized by the National Centre for Research and Development, two telescopes are built, with wide and narrow fields of view, making it possible to detect and assess the status of LEO space debris (Defence24 2016d).

The telescopes will be part of the so-called Polish sky observation system (Polish SSA System), used for defense and civil purposes. Creotech is involved in several initiatives related to space surveillance, including mapping of the space debris trajectories and NEO monitoring. A 2016 project concerned the construction of an automated space surveillance and tracking system. The program was realized within the frame of the State Defence and Security program, managed by the National Centre for Research and Development. The consortium responsible for implementing the initiative included the Air Force Institute of Technology, along with Creotech Instruments S.A. and the Military University of Technology (Defence24 2016d).

Poland has been also working on active debris removal. The PW-Sat2 project's purpose is to design a satellite to test an innovative technology of the deorbiting system. The PW-Sat2 satellite will be launched into a Sun-synchronous orbit of approx. 575 km altitude, from the Vandenberg Air Force Base in the US. Thanks to the financing obtained at the beginning of 2016 from the Ministry of Science and Higher Education, it was possible to issue a call for proposals and select a launch provider for the satellite. Innovative Space Logistics B.V. (ILS) was chosen to do this task. PW-Sat1 was deployed in 2012 and decayed from orbit in October 2014. The PW-Sat1 project cost was 500 thousand EU and was financed through ESA PECS program (Kosmonauta 2016).

The 2018 ESA budget for SSA amounts to €22.9 million. Poland participates in the optional ESA SSA program with a budget of €1.16 million in 2018 (Euroconsult 2019).

---

## Portugal

### Space and Security Budget

The country had an estimated defense expenditure of €2.874 billion or 1.52% of GDP in 2018, below the NATO guideline of 2% of GDP (NATO 2019). The Portuguese Government proposed in October 2018 that its 2019 budget would include €2.34 billion for defense, a 17.5% increase compared with the €1.99 billion spent in 2018. However, the earmarked budget for defense in 2018 was €2.151

billion. The proposed budget includes €275 million for defense equipment and €6.9 million for military cooperation. €60 million will support Portuguese participation in peacekeeping missions, with the UN providing an additional €five million (Jane's 360 2018). Euroconsult estimates Portugal's space budget at €25 million including contributions to ESA (€16.1 million) and to EUMETSAT (€6.5 million) (Euroconsult 2019). No military space budget has been identified by Euroconsult.

## **Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR)**

INFANTE is an R&D project for the development and in-orbit demonstration of technology for a small satellite, precursor for Earth observation constellations. The project's Space segment includes a low-cost and modular bus; a communications system based on software-defined radio equipped with advanced functions; a small propulsion system; deployable panels with solar arrays and antennas; SAR and multispectral camera and a payload bay for scientific experiments; and equipment for validation. The Ground segment includes the development of an innovative toolkit to fast-track assembly, integration, and testing of small satellites and a "data hub" to aggregate, process, and disseminate data. INFANTE is led by TEKEVER ASDS and puts together renowned Portuguese companies in the field of Space, such as Active Space Technologies, GMV, HPS, Omnidea, and SpinWorks, among others; internationally recognized R&D centers such as CEIIA, FCT-UNL, FEUP, INL, IPN, ISEP, ISQ, ISR Lisboa, IT Aveiro, and UBI; national partners like Deimos Engenharia, Edisoft, and Optimal; and end users such as IPMA, INIAV, or the Portuguese Maritime Authority and international organizations (Space Today 2018).

Portugal has made use of the EU civil protection mechanism, following requests for assistance to battle forest fires in the country. The Copernicus EMS Rapid Mapping has been activated by the Portuguese National Authority for Civil Protection to produce delineation (showing the extent of damage) and grading (showing the magnitude of damage) maps for Areas of Interest (Copernicus 2017).

Satellite imagery is used indirectly by the three branches of the Portuguese armed forces (AAFF) in their use of cartography and geointelligence in operational planning. Geointelligence is obtained from organizations to which Portugal belongs or through agreements or protocols with third countries or entities, including for instance SatCen. The Center for Military Intelligence and Security of the Armed Forces General Staff is the body responsible for disseminating geospatial intelligence to support the planning and conduct of military operations (IUM 2016). The Army, specifically the CIGeoE, uses satellite Earth surface imagery in the international project Multinational Geospatial Co-Production Program. This project aims to develop a global geographic information system. For that purpose, it uses high-resolution satellite imagery, from which cartographic intelligence is produced. The intelligence acquired is essentially used for support to weapons systems, military operations, humanitarian aid, and

disaster situations. The images are obtained from a protocol with the Portuguese Sea and Atmosphere Institute, which in turn obtains them from EUMETSAT (IUM 2016).

The Ministry of Environment and the Portuguese Institute of Sea and Atmosphere initiated a project to build an infrastructure for the Portuguese Sentinel data – IPSentinel. This infrastructure will allow access to the data of the Sentinel satellites of the Portuguese territory and the search and rescue area in the Atlantic Ocean under the responsibility of Portugal. The project is promoted by the General Directorate of Marine Policy through the Financial Mechanism of the European Economic Area (ICACI 2015).

Portugal is participating in the Copernicus program in the frame of the EU and ESA. Portugal contributes to ESA Earth observation programs with a budget of €1.6 million for 2018 (Euroconsult 2019).

## **Satellite Communications (SATCOM)**

The PoSAT-1 was launched into orbit in September 1993, on board the Ariane 4 rocket. The satellite was developed by several public, private, and military entities and was partly financed by the government. The program aimed to prepare the Portuguese industrial fabric to gain presence in the space industry and to promote Portugal's technological and scientific development. The PoSAT-1 was used by both military and civilian organizations until 2006. The PoSAT-1 allowed the AAF to carry out tactical and strategic communications, data transmission of encrypted and unencrypted messages, reception of images, and meteorological information. Data from the PoSAT-1 is no longer used by the armed forces, which now relies on private contractors and agreements with third countries or institutions.

Both the supreme military body of Portugal and the branches of the Portuguese armed forces contract private service providers, but only the former contracts communications to military satellites (X-band). The Navy uses military satellite communications (X-band) in the Frigates, the Submarines, and in the Replenishment Ship. Nearly all naval assets are equipped with the Global Maritime Distress and Safety System, which provides INMARSAT coverage beyond the 300-mile line. Satellite communications are particularly important to the Army and to the National Deployed Forces (IUM 2016).

Both the Navy and the Army consider satellite communications especially important for operational contexts. However, it should be noted that the Navy still relies on radio communication to ensure redundancy, even if it is only partial. The Navy also relies on the Metocmil system to ensure redundancy in satellite communications. This dependence can be seen in the several uses for data from satellite communications in Portuguese military operations outside national territory and in the use of these images for cartography and meteorological forecasts (IUM 2016).

Portugal participates in satellite communication activities through ESA's optional ARTES Programs, with a budget of €2 million for 2018 (Euroconsult 2019).

### **Positioning, Navigation, and Timing (PNT)**

The Portuguese Armed Forces (AAFF) use both civilian and military GPS signals. The Navy uses the civilian GPS signal for navigation, except for frigates, which use the P(Y) GPS signal. However, the use of PNT data is important not only to the Navy, but to maritime navigation in general. Portugal has differential GPS stations to improve the precision of the GPS signal by comparing the information received with a known location. The use of PNT data is also deemed essential to the cartographic process of the CIGeoE (AAFF Geospatial Information Centre). This process uses data from GNSS, which combines signals received from the GPS, Glonass, and, in the future, the Galileo systems. The Armed Forces use civilian and military GPS for several weapons systems, mainly for aeronautical navigation (IUM 2016). Aircraft navigation systems can be exclusively inertial or mixed. With a mixed navigation system, more technologically advanced aircraft combine GPS signal with inertial signal, thereby reducing the latter's intrinsic error and increasing precision. The civilian GPS signal is currently used for navigation in the field of Research, Development and Innovation, in the research line of unmanned aerial vehicles (IUM 2016).

Since 2006, the Ministry of Environment has been working on the densification and the upgrade of the GNSS CORS (Continuously Operating Reference Stations) network – ReNEP – with two main goals: (i) the maintenance of the national reference frames; and (ii) to provide a real-time precise point positioning service. In 2015, the Directorate-General of Territory (DGT) finalized the network, which consists of 48 CORS: 42 in the mainland and 7 on the islands (Azores and Madeira Archipelagos). All the stations collect both GPS and GLONASS data, six are part of the EPN (EUREF Permanent Network) and three of these also belong to the IGS (International GNSS Service) network (ICACI 2015).

Further, Portugal participates in the optional Navigation programs in conjunction with the EU EGNOS/Galileo flagship program.

### **Space Situational Awareness (SSA)**

At national level, SST fits into the Research and Innovation Strategy for Intelligent Specialization (EI&I) 2014–2020. It contributes to the Industrial Development Strategy for Growth and Employment (EFICE) 2014–2020, promoting better exploitation of national and European funds, and allows optimizing the fulfillment of the objectives defined in the Strategic Concept of National Defence. At the end of 2018, Portugal joined the EU SST Consortium. Portugal's participation in the EU SST program aims to build a national SST capacity, which is properly articulated with

other national programs in space, integrating sensors, processing capacity and services, currently dispersed by several entities (IUM 2016).

The Portuguese initial SST capacity was prepared in the frame of the Space Surveillance and Tracking Project Group, abbreviated GPSST. It is financed through funds entered in the Military Programming Law, in “Central Services-Joint Capabilities,” through the project “Support Defence Technological and Industrial Base (BTID).” Up to a maximum amount of €1.4 million is to be increased through the budgets of other participating entities (Portuguese Government 2017).

The Portuguese initial SST capacity provides for the installation of the National Operating Centre in the Science and Technology Park of Terceira Island (TERINOV) and also an optical observatory with two telescopes in the Pico do Areeiro – Madeira. There are additional ideas to establish a radar component on Flores and Corvo. The GPSST was tasked to provide to the Council of Ministers by the end of October 2018 the future governance model of the national SST program after its functions have been terminated, proposing its structure, identifying sources of financing for the sustainability of the national SST infrastructure, considering the possible engagement to SSA, and ensuring the necessary compliance with the 2018 National Strategy for Space (Portuguese Government 2018).

Portugal participates in the optional ESA SSA program for €133 thousand in 2018 (Euroconsult 2019).

---

## Romania

### Space and Security Budget

Romania had an estimated defense expenditure of RON 17.181 or 2.04% of GDP in 2018, matching the NATO guideline of 2% of GDP (NATO 2019). Romanian government expenditures for space-related activities amounted to RON 252.3 million in 2018, resulting from parallel contributions to ESA (RON 190.3 million) and EUMETSAT (RON 24.4 million) (Euroconsult 2019). No military space budget has been identified by Euroconsult.

### Space and Security Program

The Ministry of Education and Research funds the Research, Development and Innovation STAR Program – Space Technology and Advanced Research for the 2012–2019 period, through the Romanian Space Agency (ROSA). The program includes three subprograms: Research, Infrastructure, and Support (ROSA Website). The Science and Technology pillar of the S3 strategy of ROSA focuses on participation of relevant institutions and relevant programs. The Services pillar of the S3 strategy of ROSA focuses on participation of relevant institutions and relevant programs. The Security pillar of the S3 strategy of ROSA focuses on participation of relevant institutions and relevant programs (ROSA Website).

## **Earth Observation (EO)-Intelligence-Surveillance-Reconnaissance (ISR)**

Romania has an IMINT and GEOINT training facility in Bucharest, led by ROSA and the Military Technical Academy (MTA Website). The Geospatial Intelligence Center provides the spatial foundation essential for the analysis of information from all sources, providing the baseline starting point for all geographically referenced analytic efforts. It brings together cartography, imagery analysis, geospatial analysis, geodesy, aeronautical analysis, maritime analysis, and regional analysis in Romania, providing unique intelligence capability (MTA Website).

ROSA is implementing studies for a national EO ground and space system, including optical and radar observation facilities (EISC 2016). Romania has a Centre for Remote Sensing Applications in Agriculture, called CRUTA. Important contributors to national remote sensing activities include the ROSA Research Center, the Remote Sensing Laboratory; the Institute of Geodesy, Photogrammetry, Cartography, and Land Management; the Institute of Soil Sciences and Agrochemistry; the National Institute of Meteorology; the Geological Institute of Romania; the Military Surveying Service; the Romanian Forest Research and Management Institute; the Institute of Studies and Design for Land Reclamations; and the Institute of Geology and Geophysics (ESA 2015).

Romanian ministries are increasingly using space-based service in support of a variety of policy areas. As an example, the Ministry of Environment contracted TerraSigna, a GIS service provider, and a team of volunteering IT specialists to create “Inspectorul Padurii” (The Forest Inspector) in the frame of combatting illegal deforestation in Romania. “The Forest Inspector” is a geographic information system that can ingest radar and high-resolution satellite images from Sentinels 1 and 2, Landsat, OpenStreet, and Google Maps. The software then scans successive images of the same areas to identify changes in the forest that indicate where logging has taken place. The data is refreshed every 2 to 7 days, which enables authorities to become aware of any illegal logging in almost real time. The satellite-based map is further enriched with information coming from the government’s digital database and tracking system. Such information can include who has permits to cut what and where, what the truck’s license plate number is, and when the logging took place. Protected areas are monitored through the platform. In addition, the map can be used to identify fake GPS loading points, faster (Eurisy 2017).

Through the European Maritime Spatial Planning (MSP) Platform, financed under the European Maritime and Fisheries Fund (EMFF), the National Institute of R&D for Optoelectronics implements RO-CEO, the Romanian Cluster for Earth Observation, a project running from November 2016 until October 2019 (MSP Platform Website). The RO-CEO project aims to increase the capacity of Romanian organizations to contribute to ESA’s Earth observation programs and projects, by setting-up the Romanian Cluster for Earth Observation, a formal association of organizations, with its own statute and agenda. RO-CEO project unites key players at national level, addressing several important aspects of the Earth observation activities, to support geophysical algorithm development, calibration/validation

and the simulation of future spaceborne earth observation missions. The main roles of the cluster are: to promote the specific interests and relevant capacities at national level; to attract more investments and contracts for the Romanian institutions; to improve the provision of services to end users by joining complementary skills and expertise, and; to ensure the sustainability of the EO sector in Romania by enabling EO market development (MSP Platform Website).

Romania is advancing on the establishment of a satellite EO data reception and processing center. The National Institute of Research and Development for Optoelectronics has a Center for Atmospheric REMote Sensing and Space Earth observation. The National Institute for Marine Research and Development “Grigore Antipa” has a Space Technologies Competence Centre Dedicated to the Romanian Marine and Coastal Regions Sustainable Development. The Polytechnic University Research Center for Space Information in Bucharest has a competence center for smart sensors and big data technology for space applications (EISC 2016).

The Romanian government has depended on the International Charter on Space and Major Disasters and the Copernicus Emergency Management Service, with space-based imagery delivered to ROSA and ministerial stakeholders in the frame of national disaster management, notably triggered by floods (Eurekalert 2005).

In December 2017, ESA and ROSA signed an Understanding for the Sentinel Collaborative Ground Segment Cooperation to facilitate Sentinel data exploitation in Romania. Under the agreement, ROSA will coordinate ground segment activities in Romania – such as hosting, distributing, ensuring access, and archiving Sentinel data – and act as an interface between ESA and national initiatives. ROSA also plans to cooperate with different European partners and institutes. The Sentinel Collaborative Ground Segment aims to provide complementary access to Sentinel data and/or to specific data products or distribution channels. The collaborative elements bring specialized solutions to further enhance the Sentinel missions’ exploitation in various areas, such as data acquisition and (quasi-) real-time production, complementary products and algorithms definitions, data dissemination and access, development of innovative tools, and applications as well as complementary support to calibration and validation activities (ESA 2017).

Romania participates in ESA Earth observation programs with a budget of €4.16 million in 2018 (Euroconsult 2019).

## **Satellite Communications (SATCOM)**

The Romanian Ministry of Defence wants to launch its own telecommunication satellites into geostationary orbit as part of a strategic project, according to a press released following a meeting between the Defense Minister Gabriel Les, the head of Romanian Space Agency (ROSA), and ESA experts (Business Review 2018).

Romania participates in satellite communication activities through ESA’s optional ARTES programs, with a budget of €2.53 million in 2018 (Euroconsult 2019).



---

## Positioning, Navigation, and Timing (PNT)

Romania has a national permanent GNSS network of 74 reference stations (in 2016). The system provides GNSS augmentation services under ROMPOS – Romanian Position Determination System. ROMPOS is part of the Central and East Europe ground station augmentation system named EUPOS. ROMPOS services include DGNSS service (dm accuracy), RTK service (cm accuracy), and GEO (geodetic service – cm/mm accuracy). ROMPOS services are provided through the National Center of ROMPOS Services (NCRS), which is intended to monitor and control the GNSS stations activity for the automatic transfer of data to central data server, which are used for post-processing position determination and positioning services and products for real-time applications (EUREF 2016).

Further, cooperation is facilitated through ESA. Romania participates in the optional navigation programs in conjunction with the EU EGNOS/Galileo flagship program.

## Space Situational Awareness (SSA)

Romania is participating to ESA's Space Situational Awareness optional program since 2012, through the Romanian Space Agency. The main areas where national priorities are placed contribute to achieving ESA security objectives as stated in the SSA Program Declaration. The national SSA overall objectives are being fulfilled at the same time by rising national industry potential in SSA, especially in the fields of software development, optical, and radar technology and developing space weather science potential.

Romania's priority for SSA is the retrofitting of the Cheia Ground Station for SST purposes (ROSA 2018). The Cheia SST 32 m antenna may be refurbished and modified for mono- and bistatic radar tracking of NEO and space debris (EISC 2016).

Moreover, cooperation is facilitated through ESA and EU.

ROSA represents Romania in the Space Surveillance and Tracking Committee and organized by European Commission. In August 2017 Romania applied to be part of the EU SST Consortium. On May 31, 2018, Romania was admitted in this consortium as full member.

Romania participates in the optional ESA SSA program with a budget of 1.6 million in 2018 (Euroconsult 2019).

---

## Concluding Remarks

This chapter provides evidence of the trend toward increasing relevance for security and defense in national space and security programs in smaller European countries. In particular, this is reflected through dual-use utilization of "Space and

security,” both in its security from space and security in space aspects which are progressively contributing to further integration of space activities. Traditionally, only civilian space activities including for instance Earth observation, telecommunications, human spaceflight, space transportation, and technology development were subject of cooperation projects at intergovernmental and supranational level. Security- or defense-related space programs were kept at the national level or dealt with bilaterally or multilaterally in *ad hoc* cooperative programs. These trends demonstrate an evolution of European countries priorities from strictly civil-oriented applications to also encompassing security and defense ones. Dual-use allows the possibility to accommodate various needs with limited resources. The national space programs with security or defense dimension, in combination with the EU and ESA programs, demonstrate alignment toward the use of space for security and defense in smaller European countries. To conclude, the increasing relevance of security and defense in Europe, including the smaller European countries, to some extent could be framed as the necessity for Europe to advance civil-defense synergies and join resources in order to achieve autonomy as a global player.

**Disclaimer** The contents of this chapter and any contributions to the Handbook reflect personal opinions and do not necessarily reflect the opinion of the European Space Agency (ESA).

---

## References

- Belgian Ministry of Defense (2017) Coopération belgo-luxembourgeoise dans le domaine de la Défense, 23 November 2017
- Business Review (2018) Romania’s Ministry of Defense aims to launch its own satellites into orbit, 22 November 2018
- C4Defense (2018) Greece to lease Heron UAVs, 8 February 2018
- CAS (2018) China, Finland to enhance arctic research cooperation, 31 October 2018
- CNES (2018) Space cooperation with the Czech Republic - CNES celebrates Czech Republic’s 10 years of success in ESA, 13 November 2018
- Copernicus (2017) Copernicus EMS rapid mapping activation for forest fires in Portugal, 18 October 2017
- Czech GEO Data Portal Website, GNSS Data Portal, GNSS data portal. Available at: <http://www.czechgeo.cz/en/article/default/gnss-data-portal>
- Czech Ministry of Transport (2014) National Space Plan 2014–2019, 27 October 2014
- Czech Ministry of Transport (2016) CZ Space Catalogue, 2016
- Danish Government (2016) National Space Strategy, Denmark Government
- Danish Ministry of Defence (2016) Armed Forces, National Role
- Danish Ministry of Defence (2017) A strong defence of Denmark, Proposal for New Defence Agreement 2018–2023, October 2017
- DBEI (2018) Focus on Aerospace and Aviation – December 2018 DIAS Website, Astro – Research
- Defence 24 (2015) Optoelectronic data for Poland: Polish satellite programme and expansion of the agreement with Italy, 17 December 2015
- Defence 24 (2016a) Space plans made by the Polish Ministry of Defence. “Defined Needs” vs. Great Challenges, 16 April 2016
- Defence 24 (2016b) Poland Looks Towards Space. Satellite Programme Begins, 18 February 2016

- Defence 24 (2016c) Polish army looks to acquire rugged GPS units, May 2016
- Defence 24 (2016d) Polish space situation awareness system is being developed, 25 May 2016
- Defence 24 (2017) Satellites: concurrent design facility to be established in Poland, May 2017
- Defence News (2017) Poland to buy Lockheed-made rocket launcher, November 2017
- DTU (2018) Unique Danish satellite in orbit around the Arctic, 5 February 2018
- DTU Space Website, Geodesy and Earth Observation. Available at: [https://www.space.dtu.dk/english/research/research\\_divisions/geodesy\\_and\\_earthobservation](https://www.space.dtu.dk/english/research/research_divisions/geodesy_and_earthobservation)
- EISC (2016) Romanian space activities, presentation, October 2016
- EO Portal Website, Satellite Missions, MIMOSA and CatoSat-2E. Available at: <https://directory.eoportal.org/web/eoportal/satellite-missions/c-missions/cartosat-2e>
- EPA (2011) Climate Change Research Programme (CCRP) 2007–2013 Report Series No. 8, 2011
- ESA (2015) Land remote sensing in Romania, Presentation, 2015
- ESA Navipedia, EGNOS Ground Segment. Available at: [https://gssc.esa.int/navipedia/index.php/EGNOS\\_Architecture](https://gssc.esa.int/navipedia/index.php/EGNOS_Architecture)
- ESJ News (2018) Lasers and Space as Czech Contributions to NATO, EU, 17 October 2018
- Estonian Land Board (2015) GNSS Services in Estonia: ESTPOS as a case study, Presentation, December 2015
- Estonian Land Board Website, National Mirror site (ESTHub). Available at: <https://www.maaamet.ee/en/objectives-activities/geoinformatics/national-mirror-site-esthub>
- Estonian Marine Institute Website, Department of Remote Sensing and Marine Optics, Available at: <https://mereinstituut.ut.ee/en/institute/department-remote-sensing-and-marine-optics>
- Estonian Ministry of Defence (2019) Estonian defence budget 2019, September 2019
- Euractive (2019) Today the launch of HellasSat 4 – the advantages and Kleiddi, 5 February 2019
- EUREF (2016) National Report Romanian GNSS permanent network, presentation, 2016
- Eurekalert (2005) Disaster Charter brings satellites to bear on Romanian flooding, August 2005
- Eurisy (2017) Romania turns to satellites to crackdown on illegal deforestation; MSP-Platform Website, RO-CEO – Romanian Cluster for Earth Observation
- Euroconsult (2019) Government Space Programs – Benchmarks, Profiles & Forecasts to 2028, July 2019
- FICORA (2018) Finland to become a leader in 5G: the 5GKIRI cooperation project between Finland's largest cities supports construction of future communications networks, 1 November 2018
- FIG (2013) The performance of network RTK GNSS Services in Ireland, February 2013
- Finnish Government (2018) Prime Minister Sipilä: Finland and India have good opportunities for cooperation, 17 April 2018
- Finnish Ministry of Defence (2018) Division of Defence Spending, Defence Budget 2018, February 2018
- Finnish Ministry of Economic Affairs (2018) The 2019 draft budget of the Ministry of Economic Affairs and Employment: Further investments in innovation funding
- Finnish Ministry of Economic Affairs and Employment (2013) The national strategy for Finland's space activities in 2013–2020 – to space through Europe, global benefits and prosperity to Finland from space activities
- Finnish Ministry of Transport and Communications, Efficient deployment of satellite navigation systems in Finland – Action Plan 2017–2020, June 2018
- FMI Website, Finnish Meteorological Institute, Earth Observation Research. Available at: <https://en.ilmatieteenlaitos.fi/earth-observation>
- GNSSnet.hu Website. Available at: <https://www.gnssnet.hu/index.php?r=site%2Frealtime>
- GovSat (2016) GovSat Press Release: NATO AGS Contract Awarded to GovSat, 8 November 2016
- GovSat (2018) GovSat-1 Brochure, A new concept in secure communications, 29 January 2018
- HSO (2016) A new era of Hungary in space, 14 April 2016

- HSO Eötvös, Loránd University Space Research Group. Available at: [http://sas2.elte.hu/urfiz\\_hullamkiserletek\\_1EN.html](http://sas2.elte.hu/urfiz_hullamkiserletek_1EN.html)
- HSO BME, Department of Broadband Infocommunications and Electromagnetic Theory. Available at: <https://www.vik.bme.hu/en/departments/>
- HSO Department of Geodesy, Remote Sensing and Land Offices. Available at: <https://eurogeographics.org/member/departments-remote-sensing-and-land-offices/>
- ICACI (2015) Portugal National Report – ICA 2015, 23 August 2015
- ICEYE (2019) Two recently launched ICEYE SAR Satellites Commissioned – added to commercial constellation, Press Release, 12 September 2019
- ICEYE Website, History Timeline. Available at: <https://www.iceye.com/company/history>
- Infocom.gr (2020) Increased contributions of Greece to ESA, 3 February 2020
- Innoteka (2018) Magyar űrstratégia kell!, 4 May 2018
- Inside GNSS (2017) Poland in position for a big role in GNSS, 7 April 2017
- Invent Baltics OÜ, Study on Latvia's Participation in European Space Agency Since 2015, September 2019
- Investinestonia (2017) Turning theory into practice: the short story of the Estonian space race, March 2017
- Irish Examiner (2018a) Ireland's defence spending is lowest in Europe at 0.3% of GDP, 8 June 2018
- Irish Examiner (2018b) First Irish satellite one giant leap closer to space odyssey, 25 September 2018
- Irish Government (2017) News Service, Ireland signs Earth Observation agreement with the European Space Agency, Press Release, 13 October 2017
- IUM (2016) Space in the Portuguese Defence Sector, April 2016
- Jane's 360 (2018) Portugal proposes defence spending increase to Parliament, 18 October 2018
- Kosmonauta (2016) Polish PW-Sat2 will be launched into space at the end of 2017 on-board Falcon 9, December 2016
- Luxembourg Government (2016). [Innovation.public.lu](http://innovation.public.lu); SES (2018a) GovSat-1 Brochure, 29 January 2018
- Maynooth University (2014) 8th Irish Earth Observation Symposium, October 2014
- Metsar J, Kollo K, Ellmann A (2018) Modernization of the Estonian national GNSS reference station network. *Geodesy Cartography* 44(2):55–62
- Mononews (2019) Agreement Greece – ESA for the development of microsatellites, 26 March 2019
- MTA Website, Geospatial intelligence centre – about. Available at: <https://www.mta.ro/geoint/about.html>
- Muls (2016) De opbouw van het Galileo Navigatiesysteem, *Revue Militaire Belge*, December 2016
- NATO (2019) Defence Expenditure of NATO Countries (2013–2019) Press Release, PR/CP(2019) 123, November 2019
- NLS (2017) Finnish Geospatial Research Institute and its Department of Navigation and Positioning, Presentation, August 2017
- NORSAT (2012) International, case study: Finnish Defence Forces, 17 September 2012
- Paperjam (2018) Lancement d'un nouveau satellite en «triple win», 26 July 2018
- Planetek Italia (2017) Planetek strengthens its alliance with Polish space companies, December 2017
- Polish Government (2017) The Polish Space Strategy, 2017
- Polish Institute of Aviation (2018) Program of the Polish communication satellite – a debate at the Institute of Aviation, March 2018
- Portuguese Government (2017) Resolução do Conselho de Ministros 116/2017, 2017
- Portuguese Government (2018) Resolução do Conselho de Ministros 113/2018, August 2018
- ROSA (2018) The 3S – new ROSA strategy, presentation, September 2018
- Sagath D, Papadimitriou A, Adriaansen M, Giannopapa C (2018) Space strategy and governance of ESA small member states. *Acta Astronaut* 142:112–120

- SatelliteToday (2015) Denmark Expects MilSatCom capacity Surge to continue, 9 April 2015
- Satnews (2017) Four Additional Satellites Ordered from GomSpace A/S and Aerial & Maritime, 19 December 2017
- Schenk et al (2010) GEONAS - geodynamic network of permanent GNSS stations within the Czech republic. *Acta Geodyn Geomater* 7(1). (157):99–111
- Schrogl K-U (et al.) (Eds.) (2015) *Handbook of Space Security: Policies, Applications and Programs*. Springer, New York
- Science Business (2017) Aalto-2 satellite launched into space, 20 April 2017
- Science in Poland (2017) Polish Space Agency: Draft National Space Program is ready, 27 December 2017
- Science in Poland (2018) FP Space launches the Polish commercial satellite Intuition-1 project, 26 February 2018
- Security Luxembourg (2018) Defense – Luxembourg to buy an observation satellite, 19 January 2018
- SES (2016) SES enables Danish Defence wideband global satcom system connectivity, 12 May 2016
- SES (2018) SES Provides Managed Services for Galileo, 30 May 2018
- SIGNAL (2015) Danish Military Procures SATCOM Terminals, 7 April 2015
- SIPRI (2016) Military capabilities in the Arctic: a New Cold War In The High North?, SIPRI Background Paper, October 2016
- Space News (2017) Luxembourg eyes Earth-observation satellite for military and government, 7 November 2017
- Space R&D (2018) Polish Space Agency eyes \$420M program to develop satellites, 6 March 2018
- Space Today (2018) Microsatellite constellations from Portugal, 16 October 2018
- SpaceNews (2018) International SSA agreements could pave the way for further space cooperation, panelists said, 18 April 2018
- TaNea (2019) The confidential plan “KLEI.D.DI.” for the phones of Pavlopoulos, Tsipras and ministers, 9 March 2019
- Telespazio (2015) COSMO-SKYMED: the collaboration between Italy and Poland is strengthened, 2 September 2015
- TTU Website, TTU100 Satellite. Available at: <https://www.ttu.ee/projects/mektory-eng/satellite-programme-3/satellite-programme/>
- University of Tartu (2018) Tartu observatory develops new instruments for global remote sensing network, 17 April 2018
- ViaSatellite (2016) Denmark gains access to WGS constellation via SES anchor stations, Satellite today, 17 May 2016
- ESA (2017) Pooling and Sharing for Government Satcoms, 21 November 2017



Jean-Daniel Testé

## Contents

Introduction .....	1330
Dependency .....	1330
The Threat: Increasing Suspicious Developments .....	1332
Attack Directed Against the Satellite Itself from the Ground .....	1332
High-Altitude Nuclear Weapons .....	1333
Directed-Energy Weapons (AED): Lasers and Microwaves .....	1333
Hard Attack Against the Ground Segment .....	1333
Jamming .....	1333
Cyberattack .....	1334
Satellites Able of Making Co-orbital Spatial Rendezvous .....	1334
French Space Surveillance Capabilities .....	1334
Origins .....	1334
Organization and Capacities .....	1335
Basic Principles for Enhanced Security in Space .....	1337
First Principle: Resilience .....	1337
Second Principle: Knowledge .....	1337
Third Principle: Protection .....	1338
Fourth Principle: Action .....	1338
Next Step .....	1339
Modernization .....	1339
Cooperation Within the EU .....	1340
Conclusion .....	1342
References .....	1342

---

J.-D. Testé (✉)

OTA (l'Observation de la Terre Appliquée), Peujard, France

e-mail: [jd.teste@wanadoo.fr](mailto:jd.teste@wanadoo.fr)

---

**Abstract**

Our Western societies are increasingly dependent on space systems. These have become essential to many daily activities as well as to strategic activities of prime importance. In an international context that is currently particularly troubled, their security becomes a major issue. France has been interested in this subject for several years and has developed unique space surveillance capabilities in Europe. These means, precursors 30 years ago, must today be modernized and adapted to current risks and threats. This technical evolution will have to be carried out in coherence with a doctrinal evolution based on simple and global principles. In regard to the costs of such technical changes, the evolution shall be considered within a wide European cooperation considering that finally EU sovereignty will be largely reinforced by these systems.

---

**Introduction**

At a time when rivalry among the world great powers is spilling over to space, the safety of French satellites could be threatened, directly or indirectly. Directly, because some powers consider France as the indefectible ally of a rival power or as an autonomous entity with the ability to monitor space and therefore with the ability to reveal potential suspicious actions in space. Indirectly, because space is a particular medium where Kepler's laws dictate that an activity on a precise orbital position may have consequences to other orbits. The Indian March 27 missile shooting down a satellite in low Earth orbit is the most recent example.

Given the importance of own space capabilities for society, for efficient diplomacy, and for military operations, France cannot risk losing control. However, one realizes that we do not have today the necessary means to deter a potential adversary from conducting an action in space that could harm one or more satellites. Nevertheless, in the short term, the application of some basic principles should help to limit the consequences of this deficiency.

---

**Dependency**

For many years France has assessed the ability of the space domain supporting autonomous situational awareness and decision-making while simultaneously being a unique force multiplier in support of military operations. In this regard space is considered strategic. Today, more than 30 years after the launch of the first French military payload in space (Syracuse I Telecom payload in 1982), space capabilities have become increasingly important in the whole range of defense and security operations. We are at the turning point where military space and space infrastructures at large have evolved from necessity to dependency driven. Entering into the second decade of the twenty-first century compels us to review our space heritage from the Cold War. Almost nine billion people on planet Earth, with a growing number of major space-faring

nations and nuclear powers, pose challenges to the military who push their limits through an unprecedented series of operations. This is a new paradigm illustrated by fights in Afghanistan, Libya, Mali, Central African Republic, and now Iraq and Syria.

France is historically the third space-faring nation. After more than 50 years of dedicated vision and investments in space industry and programs, France has developed innovative and credible capabilities which ensure its independence and constitute a tangible asset contributing to the development of coherent European defense space cooperation. The main capacities the French armed forces will have to fulfill in the following years are stipulated in the 2013 French White Paper on Defense and National Security (2013 Livre blanc de la Défense et sécurité nationales): entry at first, precision strikes, special forces, and work as a framework nation within an international coalition.

Accordingly, before a “go” decision is taken, the following conditions are required:

- Prior knowledge of the theater of operations and its environment (geography)
- Precise knowledge of the enemy and forces engaged (Intelligence)
- Precise knowledge of intended targets (Targeting)
- Capacity to perform missions in complete safety and without collateral damage (precise Navigation)
- Ability to dispatch orders and assign responsibilities (Command & control)

In addition to that, modern soldiers must face three new emerging game changers:

1. The first one is *time*. Time is critical, the time of decision-makers, the time of the media, and the time of social network and globally the new cyber dimension.
2. The second is *tempo*. Operations have to be conducted fast, with visible results and limited footprint in the shrinking military capabilities and operating context.
3. And the third is *adversary*. We are facing a new kind of enemy. Indeed, its nature covers now a wide range from small terrorist groups to organizations using conventional weapons and cyberspace capabilities, easily switching from one side of the scope to the other such as Daesh or Al-Qaida.

The great news is that we are now able to fulfill all these challenges. This is only possible because we have completed a full spectrum of space capabilities:

- Observation and localization are required for geography.
- Observation and eavesdropping are necessary for intelligence.
- Observation and accurate localization enable accurate targeting.
- Navigation and SATCOM are a unique support for operations.
- SATCOM are mandatory for command and control.

The availability of all these space capabilities for all warfighters allows French armed forces to perform military operations at the right *time*, with the right *tempo*, and whatever the kind of *adversary* they have to fight against.



Space provides the fantastic leverage one needs, but on the other hand, we need to cope with the dependency on our own space capabilities without any efficient alternatives. Hence, these capabilities need to be protected and preserved at a time where more countries are experimenting anti-satellite weapons.

---

## **The Threat: Increasing Suspicious Developments**

Today we are witnessing a resurgence in the rivalry among the great powers of our world. Each of them intensifies their efforts in the space domain in order to demonstrate a mastery or even a supremacy in this strategic field. To this end, their research activities are endowed with much larger budgets than in the past, which enables them to experiment, on the ground or in orbit, with new technologies that may ultimately constitute threats or even weapons against operational orbital systems. In September 2018, the French Minister of the Armed Forces (Ministre des armées) Mme Parly gave a very specific illustration of this type of threat (Discours publics, Les discours dans l'actualité, Déclaration de Mme Florence Parly, ministre des armées, sur la défense spatiale, à Toulouse le 7 septembre 2018, <http://discours.vie-publique.fr/notices/183001732.html>).

Yet, in order to understand and anticipate potential future conflicts in space, it is essential to define the threats and the potential aggressors. There are two types of risks in space: artificial risks (collision with debris) and natural risks (disruptive phenomena related to solar activity). Although risks constitute an important concern today, we will mainly address threats here. The main difference between risks and threats lies in the intent of the latter.

Weaponization of space refers to the deployment of real weapons into orbit and no longer simply supporting systems for armed ground operations (militarization). Weaponization has been experimented since the 1960s. While the activities in this area were dominant during the Cold War, the latest significant activities date back to 2007–2009, when the Chinese and the Americans each destroyed one of their deactivated satellites to demonstrate that they had a real operational capability. Weaponization, therefore, seems to have become a credible risk with multiples shapes as presented below.

## **Attack Directed Against the Satellite Itself from the Ground**

The attack by a customized ballistic or anti-aircraft missile is feasible only against low orbit satellites. This is a precision attack that requires the aggressor to get accurate data on the orbit and missile technology with devastating consequences. The Chinese experience of firing a ballistic missile against one of its own satellites has caused an unprecedented number of debris (about 30,000). On 27 March 2019, India as well managed to successfully fire a ground-based anti-satellite weapon against a satellite in low Earth orbit (The Wall Street Journal, India Successfully

Tests Satellite-Killer Missile, 27 March 2019, <https://www.wsj.com/articles/india-successfully-tests-satellite-killer-missile-11553679166>).

## **High-Altitude Nuclear Weapons**

A nuclear explosion in space via missile, although experimented by the Russians and the Americans, is far too destructive without any selectivity and therefore a very unlikely threat.

## **Directed-Energy Weapons (AED): Lasers and Microwaves**

Low-energy lasers are a very likely threat as well because the technology is mature. They can dazzle (deny the ability to take a picture) the observation satellite and damage the components of the optical chain (degradation the quality of the image). High-energy lasers can damage a satellite's structures, including its solar panels or optical parts. This technology that requires high power is not yet fully achieved, but it is estimated that the three main space powers have experimented and are developing such weapons. High-powered microwave (MFP) weapons emitted by radiation from the ground can destroy the satellite's electronic components by creating a magnetic field. This technology is also under research and development among big powers.

## **Hard Attack Against the Ground Segment**

This attack can be targeted and is already technologically and operationally feasible. The consequences of a hard attack on the user ground segment (mission center, receiving antenna, and computer system) could disable the satellite programming and data receiving. The consequences against the control/control segment could be the disruption of communication with the satellites (in both directions). The satellites could then go out of order. An attack on the antennas (2Ghz) could prevent sending commands to the satellite.

## **Jamming**

The jamming of telecommunications and navigation signals represents maybe the most important and probable threat against space services. The technology is already well mastered, and operational concepts are very similar to those used against ground devices. The direct consequence could be to prevent or disrupt all communications and navigation. For an observation satellite, the consequence could be to render it temporarily out of service. This threat category includes also spy satellites

sometimes known as “browsers.” Spy satellites manage to get close to the target satellites in order to spy and sometimes jam their communications.

## **Cyberattack**

Cyberattacks are quite feasible and probable. Particularly complex to detect and assign, they are likely to be used extensively against ground segments of space systems even in peacetime.

## **Satellites Able of Making Co-orbital Spatial Rendezvous**

Many spacefaring nations are today interested in the ability of a satellite to maneuver on its orbit. They are conducting studies and experimenting under the umbrella of active debris removal. But these technologies will certainly allow a satellite to capture a debris and bring it out of orbit. In addition, they will enable to approach, capture, and deorbit another satellite. This threat is already part of the capabilities of the three main space powers. This inventory is certainly not exhaustive but revealing the different research activities and experiments conducted by the major space powers. Their goal is to have the ability, if necessary, to significantly reduce the advantage that satellites provide to an adversary in conflict, be it diplomatic, economic, or military.

Fully aware of the strategic capabilities of space assets, France has very early developed capabilities for space surveillance.

---

## **French Space Surveillance Capabilities**

### **Origins**

French military capabilities for space surveillance have their origin in national nuclear deterrence. Indeed, given the very high level of availability and security required, training of ground operations and armed forces at times had to take place out of the sight of countries potentially affected by these capabilities. That is to say, undetected by their means of gathering information and, in particular, by observation and eavesdropping satellites.

The easiest way to avoid being detected by an intelligence satellite is certainly to operate out of range of it at the time when they are far from the area of operations. It is therefore essential to know their orbits with great precision. Although initially the orbital data of the enemy satellites were provided to the French Defense by North American Aerospace Defense Command (NORAD), it quickly became clear that such dependence was not consistent with the need for total sovereignty of France’s deterrent capability.

Thus, in the 1980s, the Direction générale de l'armement (DGA) and Office National d'Etudes et de Recherches Aérospatiales (ONERA) developed capacity demonstrators in various fields, radar surveillance, optical surveillance, and electromagnetic listening:

- The Grand Réseau Adapté à la VEille Spatiale – Grand Network Adapted to Space Surveillance (GRAVES) space surveillance radar which allows the creation of a catalog of space objects and their orbital characteristics in complete independence
- The Systeme Probatoire d'Observation du Ciel (SPOC) which could complete and specify the catalog of GRAVES
- An eavesdropping antenna to determine the activity of space objects

Although the GRAVES radar was put into operational service in the armies in the early 2000s, the other two systems remained at the demonstrator stage.

This brief historical reminder of the origins of the surveillance of the military space in France makes it possible to explain the current limits. In fact, the performances specified in the GRAVES system were to be able to detect and track the foreign observation and listen to satellites (at the time of spacecraft weighing more than 1 ton, measuring more than 1 meter, and orbiting between 300 and 1200 km altitude).

## Organization and Capacities

In addition to its performances, which are still unique in Europe, the GRAVES radar also had motivated the French Defense to organize itself in order to implement this new system and get the best benefit from it.

The system was entrusted to the Air Force and more particularly to the Command of Air Defense and Air Operations (CDAOA) which operates from the air base of Lyon-Mont Verdun. The unit in charge of this activity is COSMOS (Operational Center for Military Surveillance of Space Objects).

For the great benefit of the armed forces, the COSMOS mission is therefore to implement space surveillance sensors, to manage the national catalog of space objects, to detect abnormal behavior, to provide space support for military operations, and to manage the space meteorology. In the event of abnormal behavior, security risk, or spatial danger, COSMOS is also responsible for disseminating the alert and informing the authorities.

In addition to the GRAVES radar, the COSMOS also implements SATAM radars which are very accurate and can specify the orbitographic data of the catalog when it is particularly necessary (e.g., calculation of avoidance maneuver). Finally to monitor distant orbits (median or geostationary), the COSMOS has access to the GEOTRACKER system and can program CNES TAROT telescopes.

In 2008, the White Paper on Defense and National Security recommended that “the doctrine of space operations and programs be placed under the responsibility of

an identified and dedicated joint command under the authority of the Chief of the Joint Staff.” As a result, the Joint Space Command (CIE) was created in 2010 to develop and implement the French military space policy.

In its current form, the CIE exercises only a simple coordination of national space activities. With the exception of the field of international relations applied to the military space in which he is the leader, under the control, however, of the international relationships division of the Joint Staff, the CIE has no command. Its responsibilities are at best shared at worst, attributed to other military organizations.

The preparation of the future and the space programs are conducted by the CIE under the kind control of the Deputy Chief of Staff Plans of the Armed Forces. Military Intelligence Directorate (DRM) and Information Systems Directorate (DIRISI) have full authority, respectively, over the observation and telecommunications space systems. Authority over space surveillance activities is shared with DRM and CDAOA. The DGA and the CNES exercise all their authority over prospective studies and R&D activities. Faced with these Defense heavyweights, the CIE’s room for maneuver is very narrow.

Nevertheless, following space events in recent years concerning French military satellites, the Ministry of the Armed Forces became aware, on the one hand, of the dependence of military operations on space support and the vulnerability of the space component of Defense on the other hand.

On 13 July 2019, the President of the Republic affirmed the position of France by recalling that space is “essential for our operations” and that “by the incredible potential it offers but also by the conflicts that ‘it raises’, it ‘is [...] a real stake of national security.’” During this speech he asked for the drafting of “a defense space strategy” which “will also have a vocation to be applied, in all relevant aspects, at European level” (France 24, Macron announces creation of French space force, 13 July 2019, <https://www.france24.com/en/20190713-macron-france-space-force>).

As a result, a new national Defense space strategy is being developed. It should be published this year and restore the military space necessary dynamism to meet the challenges of security in space and give the CIE a real role of commander of French military space capabilities.

As detailed above, the majority of French space surveillance capabilities date as early as the 2000s and therefore require urgent modernization in order to be adapted to the new international space context.

The latter is characterized by a drastic reduction in the size of space systems in orbit and the development of threats against operational satellites by the majority of space powers.

It is no longer a matter of simply monitoring the space; it is also necessary to be able to guarantee the safety of our satellites.

The effort will be tremendous both financially and in terms of human resources. The Ministry of the Armed Forces will have to make choices, and they will be dramatic since they are not anticipated: more space will certainly mean less of one (or more) other capacity. The new capacities will have to be developed in respect of the principles detailed below.

## **Basic Principles for Enhanced Security in Space**

### **First Principle: Resilience**

Resilience is the ability of a system to react to a disturbance, to reorganize itself, and to continue to operate in the same way as before the disturbance. In terms of military space, resilience makes any attack on the resilient system particularly difficult or even ineffective. In addition to hardening the space systems involved, which makes them more expensive and heavier, resilience can be achieved by dispersing the single satellite function across multiple systems, a solution called distributed architecture. For example, a telecommunication satellite constellation is a distributed architecture solution, which makes this telecommunication system particularly difficult to disrupt since several satellites in the constellation would have to be destroyed in order to significantly degrade the system's capacity. Furthermore, a constellation of small satellites with spare satellites has a greater capacity for easy renewal than a single large satellite, which further increases this resilience.

The USA has perfectly integrated this distributed architecture concept since they have found on the one hand their dependence on space systems and on the other hand the fact that the geostationary orbit is no longer invulnerable. By focusing on the very design of the system, they provide a relevant answer, reliable, efficient, and less expensive than other solutions.

The distributed architecture concept can also apply to other aspects. One of them is to disseminate a same capacity on several systems between several allied countries (observation, GNSS, communication). For example, the Galileo and GPS systems both provide a GNSS signal, so it is possible to subscribe to both systems and thus have continuity of service if one of them is unavailable because of disruption by unfriendly country or enemy.

The principle of resilience is thus a first step toward what could be called "spatial deterrence." Indeed any act of destruction of any spatial capacity would de facto create a "deterrent" cost both financially and diplomatically. The next step to be fully deterrent is the ability to identify the aggressors without any doubt.

### **Second Principle: Knowledge**

"To know how to defend oneself, one must first know against what to defend." As such, two deadlines need to be considered.

In the short term, the regular monitoring of the enemy's behavior will allow to understand his tactical approach and to decode his strategy. The intelligence work is essential to decode the enemy's behavior and to anticipate it. It is primarily founded on the surveillance function that is to say the regular monitoring of activity in space. The major space powers of the world perform this watch using both terrestrial means (radar, telescopes) and space means. Then the spatial situation has to be elaborated and constructed from the analysis of the movements of space objects to detect any potential threat; this is what is called the SSA (Space Situational Awareness).

Although France is one of the few nations to have developed this capacity, it remains very modest compared to the major space powers and must now be modernized and improved through a real ambitious SSA capacity procurement plan.

Later, the technologies changes will bring out new capacities that will have to be taken into consideration. Thus the electrical propulsion applied to space (of low thrust but of very high yield) makes it possible to board masses of propellant 6 to 20 times lower, thus allowing greater maneuvering in space. This technology, combined with the rapid development of robotics and coupled with artificial intelligence, will enable friendly or unfriendly automatic space appointments. These developments make it even more necessary to update our surveillance capabilities so as not to be threatened and defenseless.

Above all, it is first and foremost a question of technological foresight and operational innovation by developing a clear vision of the strategic objectives in this field. With regard to the latter, its horizon of deployment, and our own scientific and technological capabilities, our political ambitions, and the importance given to our autonomy of appreciation and action, it will then be possible to define areal space strategy and to develop the technical, financial, programmatic, and operational means to implement it.

### **Third Principle: Protection**

On the one hand, protection is performed by the detection of the hostile activity then on the other hand by the security of the threatened satellite (self-protection or maneuver). If anticipation makes it possible to know what the possible aggressions are, it is necessary to detect the attack, which is complex to realize in orbit. That is why the capacity of self-protection of a satellite becomes essential regarding the emergence of the nano-satellites particularly difficult to detect from the ground. Today self-protection systems on board or fly-by are being tested in the USA; they are an effective means of detecting the threat, without having to monitor all the orbits. Such systems deserve to be developed and should be fitted at least on any satellite.

In the event of detected hostile activity, the priority will be to put the targets in security, out of reach of the attacking systems. Maneuvers can be calculated and commanded from the ground stations based on the information collected by our space surveillance systems and taking into account the knowledge gained about enemy modes of action. Subsequently, self-protection systems will enable our satellites to respond autonomously to the threat.

### **Fourth Principle: Action**

The best way to deter an enemy from attacking our space systems is to let him know that we have the means to deal with his own satellites in comparable or even greater losses. These means of action must make it possible to conduct offensive operations

similar and proportionate to the attack. This is why it is essential to have a complete panoply to act on the ground, from the ground, or completely in space.

As deterrence is concerned, a proper communication campaign should be designed to demonstrate capabilities to potential adversaries but also reassure allies and neutral countries that EU will fulfill its international commitments in terms of regulation and space law (no weaponization of space, no production of space debris).

Starting today, without developing any additional specific means, it may be possible to respond to an attack in space by targeting the ground infrastructures of the enemy's space systems. He must feel that we know the precise location of these vital centers for the implementation of its space component (space communication networks, satellite control centers, space command center, etc.), just as we have conventional weapons to destroy them by many means (operations in cyberspace, electromagnetic jamming systems, air-to-air or naval cruise missiles).

In order to broaden our field of capacities and to be able to better adapt our response, we need to have, in the medium term, systems of action from the ground to the space such as lasers, directional jammers, and microwaves weapons.

Finally, in the long term, it will be necessary to develop new capacities such as active systems in space, using new technologies and with disruptive courses of action.

Once we will master all these new kinds of operations, we will be able to deter an enemy from attacking our space systems and thereby continue to use them for the benefit of our society and the effectiveness of our diplomacy and military operations.

---

## Next Step

### Modernization

In direct connection with the new Defense Space Strategy sought by the President of the Republic, modernization of current capabilities is the challenge of the coming years.

As it has already been written, it will have to go far beyond the simple replacement of the current obsolete systems. It will, first of all, be a question of extending the knowledge of space activity to the totality of the exo-atmospheric space: from low orbits (200 km) to geostationary orbit (34,000 km).

National sovereignty in this strategic area is obviously sought, so it will be necessary to be able to unambiguously identify each of the space objects in orbit. This ability is certainly the most complex to acquire and therefore the most expensive. Two different paths are usually taken to achieve this:

- The first, the least complicated but also the least accurate, is to be able to detect each new space launch and then to follow the new object since its separation from the launcher until it goes into operational orbit. The space object is thus registered in the catalog and assigned to a country, but its mission and its performances remain however to be determined by other means of intelligence. This method



requires a surveillance system capable of detecting and tracking space launches, which is then supplemented by a space monitoring device.

- The second most accurate but more complex is to make very high-resolution images of the object and then determine the nationality, mission, and performance by image analysis. This method requires accurate, high-performance, ground-based, or deployed in-orbit imaging systems.

Combination of both methods is possible, extremely powerful, but also extremely expensive.

In accordance with the principles set out in the previous chapter, knowing the activity in space is not enough to guarantee the safety of satellites; it is now necessary to be able to protect them. The first step in this direction will be to equip them with self-protection devices, in order to detect the threat, to characterize it, to signal it, and to plan an emergency evasion maneuver. Next-generation satellites should have such devices.

A first action capability in space or to space should also be programmed. The latter is essential to the credibility of the overall posture. Indeed, how to deter an adversary from attacking our space systems if we do not have the ability to make him fear a self-defense as powerful as his attack?

The form of this component remains to be determined, certainly according to the available financial means but especially in respect of the international commitments of our country. From the ground up, the first capability that comes to mind is laser illumination to disrupt or even destroy the electronic devices of an opposing satellite. It is already technically accessible. In space, we have been mastering for several years the technique of orbital rendezvous; the conception of a space system of interception or close investigation is conceivable in the medium term and should be decided if the evolution of the nearby threats of our satellites is precise.

Finally, all these new and renovated capabilities require a command system dedicated to space. It will have to be designed in order to connect the different actors and systems of the SSA (Space Situational Awareness) chain of the Armed Forces, to provide the essential elements for the decision-making of the higher national authorities.

Sensors on the ground and in space, self-protection of the satellites, capacities of action in or toward space, and the effective realization of all these components are certainly necessary but out of reach of a budget of the Defense already under-equipped to answer the needs of deterrence and traditional components. It is therefore only at the European level that these capacities can be developed.

## **Cooperation Within the EU**

However, since its origins and regardless of the field concerned, the European Union has never accepted the leadership of a single country being an expert in the field. Thus, the development of all the necessary capabilities for European sovereignty in space cannot be properly initiated and carried out relying solely on a coalition of ad

hoc political wills. Several methods and modes of governance can lead to the result; those that seem to the author the most relevant are described below. In any case it will be necessary to convince to share an already late awareness and to mobilize competences, budgets, and efforts to reach a satisfactory result within operationally acceptable but realistic deadlines.

The first method is that of the Space Surveillance and Tracking (SST) program, based on a limited number of participants, who organize themselves to share governance and thus the allocated budget and responsibilities. The top five countries were Germany, Spain, Great Britain, Italy, and France. The initiative seemed ambitious and seductive, but it proved itself quickly unproductive. Its main weakness was to disregard the existing capacities demonstrated by each of the participating countries which led to an equal share of budgets between each and finally to a general disappointment. Indeed, countries that need to modernize their capacities (France and Germany) have not received enough European budget to achieve this. The countries without capacity (Italy and Spain) and wishing to invest to acquire one were on the other hand overbudgeted but unable of using usefully the allocated amount. As for Britain, as usual, it tried to place itself, unsuccessfully, as a referee above the fray. Failure is proven and this method of governance has now to be avoided.

A second possible method would be to attribute the realization of a first European capacity to the only two countries with developed means and experience in that field, Germany and France. Then it will be up to these two nations to agree to modernize their capacities and bring them into coherence with one another in order to achieve the complementarity required to satisfy the most urgent needs. However, it will be necessary to obtain prior approval from all other member countries and for this to give guarantees of service availability to all, knowledge and know-how transfer to those who would later be interested, and finally plan in the medium term, the creation of a true European space security center, different from the European Union's satellite center, which will have to remain focused on image analysis.

The third method that the author envisions and which he advocates will begin with an objective inventory of what exists in Europe (capabilities, services, know-how, and experience). Countries and companies offering real guarantees will then be audited to contribute to the creation of the European space security capability. Complementarity should be sought and redundancies eliminated. The European External Action Service could be responsible for this work in order to eventually create a European Space Operations Center (EOC) or EUSpOC (EU Space Operations Center).

Here is a possible agenda:

1. Inventories of existing capacities in the states of the European Union (radars, telescopes, catalogs, databases, operations centers)
2. Inventories of the commercial services of the space domain
3. Choice of capacities/services to be selected for the first European component
4. Establishment of the European Space Operations Center
5. Constitution of European capacity (connection of selected systems/services)

6. Constitution of the European catalogue of space objects/transfer of know-how to voluntary member countries
7. Review of necessary upgrades/additions
8. Achievement of selected improvements involving new actors

At the end, the European Union could be endowed with space security capabilities at the height of the protection of its space assets.

As already said the last method has the author's preference because it is the one that will allow the best taking into account the existing capabilities in each of the European countries while allowing a transfer of know-how to new players wishing to contribute to the European capacity. Governance, provided by the EEAS (European External Action Service), will overcome the risk of hegemony of large countries on the project and facilitate the involvement of new ones. Finally, the support and then the adhesion of all will be much easier to obtain.

---

## Conclusion

Like other countries in the European Union, France has developed extremely powerful satellites to ensure its sovereignty, its independence, and its autonomy of appreciation of situation and decision. In a desire to strengthen its political component, the European Union has done the same. As a result nowadays, the European society, like the other Western societies, is dependent on space for its daily functioning, security, and defense. Current space systems, although essential, are fragile and almost unprotected in space. At the same time, the main space powers are experimenting anti-satellite systems increasingly efficient and elaborate.

We must take into consideration this trend and deploy a real capacity of spatial deterrence. Since the advent of nuclear weapons, the term deterrence has been reserved exclusively for the corresponding doctrine. However, if we want to maintain the control of the use of our space systems regardless of their application, it is now necessary to deter the countries that equip themselves with systems to attack our satellites either by spying, scrambling, deception, or even more coercive actions. If it is already possible to operate in space at a low level, the acquisition of this deterrent capacity will take time and a lot of money. Acquisition of a full and independent capacity will be possible only at the European level, distributing services to all member states. This is the price to pay for ensuring the security of EU Space component, essential for European independence and sovereignty.

---

## References

- République Française, The French White Paper on Defence and National Security 2008 (Le Livre blanc sur la défense et la sécurité nationale), 17 June 2008
- République Française, French White Paper on Defence and National Security 2013 (Le Livre blanc sur la défense et la sécurité nationale), 29 April 2013



# Italy in Space: Strategic Overview and Security Aspects

# 66

Francesco Pagnotta and Marco Reali

## Contents

Introduction .....	1344
Space in Italy .....	1345
The Origin .....	1345
History .....	1346
Recent Past .....	1347
New Governance in Italian Space and Aerospace Sector .....	1347
From Operations to Applications .....	1349
Launchers .....	1349
Satellites .....	1351
Ground Segment .....	1353
From Upstream to Downstream, Through Midstream .....	1355
Space Security .....	1356
Space Security .....	1356
Space Threats .....	1357
Space Surveillance .....	1358
Cyber Threats .....	1359
Policy, Priorities, and Strategy .....	1359
New Policy .....	1359
Pillars .....	1361
Priorities .....	1362
Needs for a Strategy .....	1362
Conclusions .....	1363
References .....	1363

---

F. Pagnotta (✉) · M. Reali

Presidency of the Council of Ministers – Office of the Military Advisor, Rome, Italy

e-mail: [F.Pagnotta@governo.it](mailto:F.Pagnotta@governo.it); [M.Reali@governo.it](mailto:M.Reali@governo.it)

---

**Abstract**

Space is relevant for humankind. This is more than a concept to be agreed upon or not; it is a fact. People on Earth rely on space capabilities, applications, and services more than in the past, and it is quite impossible to think of “a day without space.” Italy has a very long history and heritage in the space sector. Starting from the period of the “space race,” Italy researched and developed technology, systems, operations, and applications over the years, and today, Italy has national telecommunication and Earth observation systems, participates in the main space-related international organizations, and has very strong bilateral collaborations in the space sector. Considering the aforementioned, Italy recognizes that the space domain is becoming more and more congested, contested, and competitive. Therefore the need for a space security program is one of the pillars in the national strategy.

---

**Introduction**

Space in Italy begins at the end of the 1950s with a team of researchers and operators from both academic and military sectors. Space activities came out of the pioneering phase faster than expected. Just after the last century, the space sector entered into a period of rapid growth.

Today, space applications and services are an integral part of daily life. If we think about the weather, communication, or navigation, each smartphone can integrate them. Earth observation, telecommunication, and navigation systems are essential in order to provide support to people on Earth, for both civil and military activities.

Key factors of this increasing relevance of space activities and capabilities are high technology, miniaturization, big data, and digitalization. These are just some of the many aspects supporting the transition to a new era in the space domain. In 2012, the USA proposed a scenario for the space domain in 2025: congested, contested, and competitive. This scenario seems to have arrived about 5 years earlier than expected. Some international initiatives, at both American and European level, have been proposed to foster the cooperation and the exchange of data and information among countries. Safety and security of “access to” and “operations in” space seem to be the most relevant topics in decision-making at the higher levels.

Today, space capabilities are essential, and their unavailability is considered more and more as a distress. It represents a vulnerability, and any similar ground-based capability cannot replace it. Therefore, in the last years, it is necessary to have a clear and shared space security strategy in order to mitigate the natural and human-made threats in and from space. Space Situational Awareness, Space Traffic Management, Cyber Threats, and Cyber Security are some of the critical topics, and they are currently under discussion in most of the international space fora.

We can easily affirm that space and aerospace are interdisciplinary sectors where scientific and technical aspects merge with socioeconomic, political, and regulatory

aspects, and we need to integrate them adequately. This leads to the adoption of a comprehensive approach in space, which takes into account all aspects and optimizes the use of capabilities according to the availability of funds at both national and international level. Finally, we have to consider that any applications and operational services support both civil and military operations. This underlines the relevance and opportunity to apply a comprehensive approach as well in the research and development of new technologies and capabilities, in order to build systems based on needs from both civilian and military field. The coordination between all stakeholders and actors – at both national and international level – becomes a key factor in the space and aerospace sectors, in order to find synergies, to encourage the development of new initiatives for international collaboration, and to support new financial means.

In this spirit, talking about new trends and markets, the commercialization of space deserves a particular mention. Initiated in the USA to facilitate and support funding from private entities in the space sector, this new trend is growing faster and faster all over the world. In Italy, in 2016, a space economy strategic program was approved with the objective to merge old and new funding lines, based on public and private support. This is a really new trend in all Europe, trying to move from the old business model, based on institutional investments to the new one based mainly on the private investments for the procurement and public investments for the services.

During the 11th Conference on European Space Policy, held in January 2019 in Brussels, the European Parliament and the European Space Agency mentioned the new “European space economy.” The objective is to establish a new space market not only limited to institutional customers but also open to private and commercial sectors. This is something similar to the Italian public-private partnership that has been used during the last 10 years, with reference to the procurement of national space systems (e.g., SICRAL 1B satellite).

---

## Space in Italy

### The Origin

In the beginning of the 1950s, Italy recognized space as a strategic domain. Space assets, satellites, and orbital platforms were equipped with the latest technology.

In 1964, Italy was the third country to conduct the launch of a satellite (United Kingdom, with the launch of Ariel 1 in April 1962, was the third country to operate a satellite, and Canada, with the launch of Alouette 1 in September 1962, was the third country to build a satellite.), the San Marco 1, with the aim to study the lower atmosphere within the framework of collaboration between the Aerospace Research Center of the University of Rome and NASA. This was just the first of a series of satellites since 1967, taking place at the United States Wallops Island Flight Facility base in Virginia (USA) and launched from the base at the Italian center of Malindi in Kenya.

## History

After more than 50 years of space history, today, Italy is at the frontier of research and technology in space.

The knowledge and experience in space has been increasing in most of the areas of the space domain: satellites manufacturing, launch and operation, launchers, enabling technologies and equipment (antennas, rockets, etc.), telecommunication and earth observation, human spaceflight and exploration, and ground segment.

Academic research and support to military and civilian operations have mainly been the triggers the rapid growth in space technologies. These two factors enabled the most of the technologies and lead to the miniaturization of electronics and structures in order to fit the stronger requirements of both military and civilian assets.

Starting with the San Marco 1 launch, Italy has developed a scientific and industrial background leading to over 100 space missions. Among others we can mention the participation to the International Space Station with astronauts, experiments, and the Italian Multi-Purposes Logistic Modules and the scientific missions like Cassini-Huygens, Rosetta, Mars Express, Hipparcos, and BeppoSAX.

International cooperation played a key role in this “Italian space adventure.” Italy is a member of the European Space Agency and collaborates with most of the space agencies all around the world: the National Aeronautics and Space Administration (NASA), the State Space Corporation ROSCOSMOS, the China Manned Space Agency and China National Space Administration, and the Japan Aerospace Exploration Agency (JAXA) are just some of the collaborations in place. In this context, space diplomacy is considered vital in order to face global challenges and research in space in a collaborative approach.

After the launch of the first national satellite, San Marco 1, the Italian scientific and industrial community worked together in order to develop other and more complex space systems. Today we have in Italy a complete chain of products in the space sector. The first Italian launch site was located near the coast of Malindi (Kenya), a floating launch site composed of three platforms where an Italian team launched 27 rockets and 9 satellites (with an American launcher, the Scout B) between 1967 and 1988. The launch platform was named San Marco, and the other two platforms – power support and control room – Santa Rita 1 and Santa Rita 2.

In 1977, the first Italian telecommunication satellite (Sirio) was launched from Cape Canaveral. In 1988, the Italian Space Agency together with the Italian manufacturing and scientific community started to realize more and more national missions. In 1991, the second Italian telecommunication satellite was launched (Italsat 1), and just 1 year after, in 1992, the first Italian astronaut (Franco Malerba) operated the Italian mission named Tethered from space.

In 2007, Italy joined the challenge of building a European navigation system: Galileo. In 2011, the first two satellites of the constellation were launched (Giove A and Giove B), and today, the constellation is operational, and two more satellites are planned to be launched in 2020.

In 2007, Agile, an Italian satellite for gamma ray evaluation, was launched, and after 5 years, in 2012, the first launch of the European VEGA launcher was conducted. The studies and the development of the launcher were carried out by the European Space Agency, and the prime contractor was an Italian company. Within 20 years, the Italian Space Agency became a significant player in the world in developing satellite technologies and mobile systems for exploring the universe and space science.

## **Recent Past**

In the recent past, the main players concerned in space were the Ministry of Education, University, and Research and the Ministry of Defence. The promotion, development, and dissemination of scientific and technological research applied in the space sector, including coordination and management of national projects and Italian participation in the European and International programs, were in charge of the Italian Space Agency, within the Ministry of Education, University, and Research. The Joint Defence Staff, within the Ministry of Defence, was in charge of military exploitation of space, including related research and development activities. The Defence was in charge of space operations and responsible for planning, coordinating, and supervising technical and operational space-related activities in support to military operations, including the homeland security aspects.

The political coordination of space-related topics was in charge of the Ministry of Foreign Affairs and International Cooperation, with the supervision of the Presidency of the Council of Ministers, through the Office of the Military Advisor to the Prime Minister.

## **New Governance in Italian Space and Aerospace Sector**

The space and aerospace sectors have been recently reorganized with the Law 11 January 2018, n.7, which reshapes the governance of national space policies. This Law, at the forefront of the European context, gives to the President of the Council of Ministers top management, general political responsibility, and coordination of the Ministries' policies relating to space programs. The Law establishes an "Inter-Ministerial Committee for Space and Aerospace policies," in which 12 Ministers (Defence; Interior; Cultural Heritage and Activities and Tourism; Agricultural, Food and Forestry Policies; Education, University and Research; Economic Development; Infrastructure and Transportation; Environment and Protection of Land and Sea; Foreign Affairs and International Cooperation, Economy and Finances; South; European Affairs.) and the President of the Conference of the Regions and the Autonomous Provinces participate.

The Law reconfirms the strategic importance of the space sector to support and enhance the economic, social, and industrial development in Italy. In particular, the



new Law has conferred to the Prime Minister the general political responsibility and the coordination of the Ministries' space programs.

Upon invitation, the President of Italian Space Agency participates in order to provide technical and scientific support. The Military Advisor to the Prime Minister was appointed as Secretary, in charge of the activities of support, coordination, and secretariat of the Inter-Ministerial Committee.

The Committee was created in order to ensure the guidance and coordination in space and aerospace sectors with reference to related operational services.

The Committee, with the modalities defined by its own internal regulation adopted in its first session and taking into account the guidelines of the national foreign policy and the European Union's space and aerospace policy, has many tasks; some of those are:

- Defines the government's guidelines on space and aerospace with reference also to research, innovation, technology, and impact on the production sector
- Directs and supports the Italian Space Agency in the definition of international agreements and in relation with international space organizations
- Ensures the coordination of programs and activities of the Italian Space Agency with the programs and activities of central and peripheral administrations
- Identifies the main guidelines for participation in the European programs of the European Space Agency and for the development of bilateral and multilateral agreements
- Defines the guidelines for the development of synergies and cooperation in the space sector between research bodies, public administration, universities, and companies, with particular reference to small and medium-sized companies in the sector
- Defines the framework of the financial resources available for the implementation of space and aerospace policies, according to criteria for the promotion and development of innovative satellite services of public interest, pursuing objectives of synergy between public and private resources, destined for the creation of space and aerospace infrastructures.

The Secretary is also the Chairman of a Coordination Board, established in order to analyze the dossiers, propose solutions to the political forum, and verify that the activities are in accordance with the political guidelines, provided by the Inter-Ministerial Committee. The Coordination Board is a Technical forum where the representatives of the 12 Ministries, the Conference of the regions and the Italian Space Agency coordinate and define the national positions for the space and aerospace programs and policies, for the approval of the Inter-Ministerial Committee. The main tasks of the Coordination Board are as follows:

- Coordinate and define the national positions, presented by Italian delegates in the European Union, European Space Agency, and in bilateral cooperation
- Implement the Inter-Ministerial Committee's decisions

- Elaborate studies and evaluations for the space and aerospace sector
- Finalize proposals and documents for the approval of the Inter-Ministerial Committee

The representatives of the 12 Ministries and the Conference of the regions (as delegates of the Inter-Ministerial Committee) take part, together with representatives of the Italian Space Agency, in the Coordination board, as permanent members with voting rights.

The Departments for Civil Protection, Regional Affairs, Cohesion Policies, Intelligence, and the Italian Institute for Environmental Protection participate, without voting rights, in the meetings of the Coordination Board.

In addition, representatives of industrial associations, industries, academic institutions, and research entities may be invited as technical consultants, based on opportunities and depending on the agenda of the meeting.

---

## From Operations to Applications

### Launchers

From past experience starting with the Scout B launches in 1988, Italy conceived the VEGA project; a launcher based on the Zefiro motor for the European Ariane program and developed by the Italian industry Bombrini Parodi Delfino.

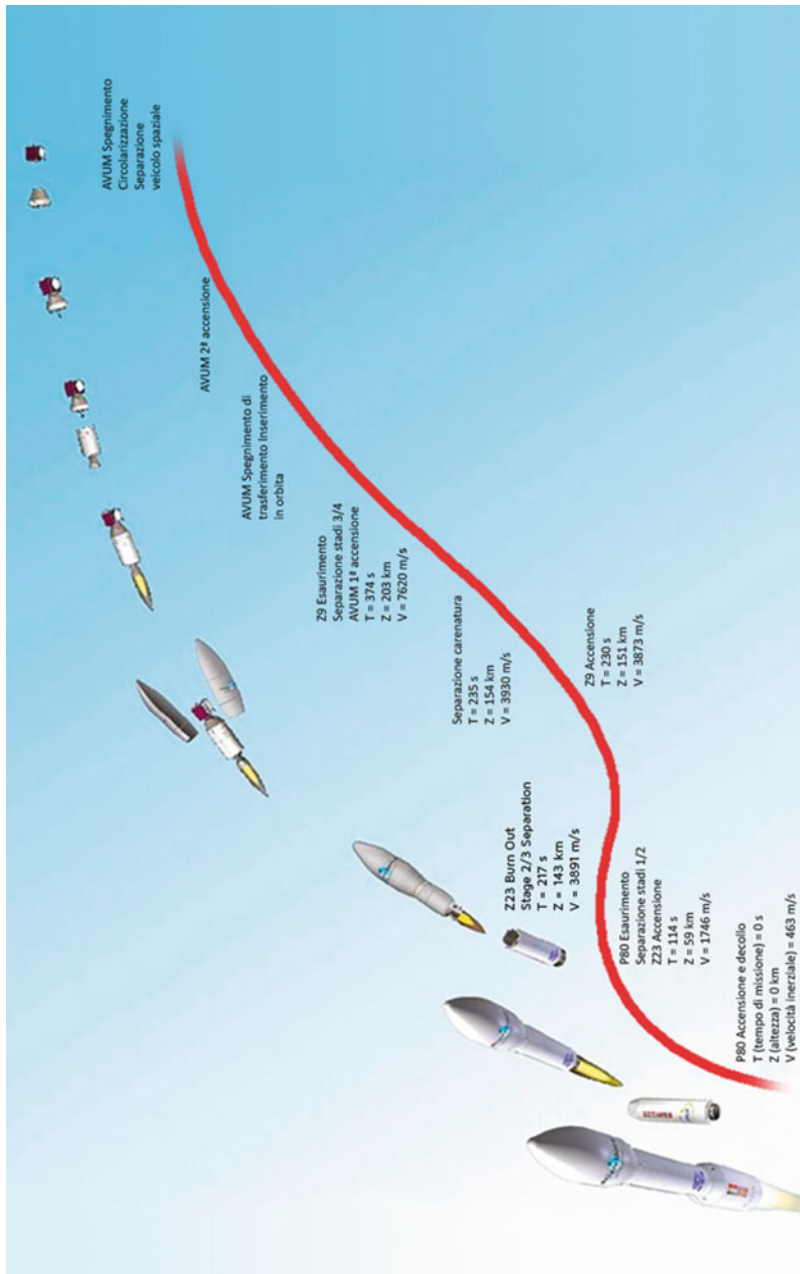
VEGA (Italian acronym for Advanced Generation European carrier Rocket) is an expendable launch vehicle, developed by the European Space Agency in 1998. The first launch took place in 2012 from the French Guyana Space Center.

Vega is a single-body launcher with three solid rocket stages (named P80, Z23, and Z9, respectively, the first, the second, and the third stage) and an upper liquid rocket stage (named AVUM). The payload range is from 300 to 2,500 kg satellites to polar and Low Earth Orbit (LEO). The reference mission is a polar orbit with 1,500 kg satellite at 700 km.

Italy is the leading contributor to the VEGA program, with 65%, followed by France with 13%, and other participants with 22%, including Spain, Belgium, the Netherlands, Switzerland, and Sweden.

The development costs for the launcher were about €710 million, with spending an additional €400 million to sponsor five development flights between 2012 and 2014. On 14 February 2012, VEGA carried out the first launch, and, today, it placed in orbit more than 20 payloads into orbit, including small satellites (Cubesat), the Intermediate eXperimental Vehicle, a part of the SkySat constellation by Terra Bella of Google, the experiments on gravitational waves Lares, and Lisa Pathfinder.

VEGA can be considered as a great success for both Avio and the over 40 European companies that contributed to the project (Fig. 1).



**Fig. 1** VEGA launch mission profile scheme – Credit: AVIO S.p.a

## Satellites

### Telecommunication

After the launch of the first Italian telecommunication satellite, Sirio, Italy began the development and launch of a series of national satellites: Italsat 1 (1991), Italsat 2 (1996), managed by the Italian Space Agency and not operational so far, the military SICRAL 1 (2001), SICRAL 1b (2009), and, in cooperation with France, SICRAL 2 (2015) and the dual-use ATHENA-FIDUS (2014) (Fig. 2).

The SICRAL (Italian acronym for Italian System for Secure Communications and Alerts) is the national system (three satellites are operational) for military communications, providing interoperability between the networks of defence, law enforcement, and civil emergency support to the management of strategic infrastructure. The program is divided into three phases, and the third one started in 2015 in cooperation with France. The system, starting from 2001, provides communication in UHF, SHF, and EHS/ka bands, anticipating the needs of growth and development in the next few years.

The SICRAL control team operates from the SICRAL Joint Control Center, located in Vigna di Valle (Roma), with a backup center in the civilian “Piero Fanti” Space Centre in Fucino (L’Aquila).



**Fig. 2** SICRAL 2 artistic view – Credit: Telespazio S.p.a

The ATHENA-FIDUS satellite (Access on THEatres and European Nations for Allied forces – French Italian Dual-Use Satellite) is a French-Italian telecommunications system, developed as a part of a collaboration between Italian and French space agencies and the Ministries of Defence. The satellite complements some capabilities already offered by the Syracuse and SICRAL systems in EHF and ka bands. The ATHENA-FIDUS is operated from a French control center.

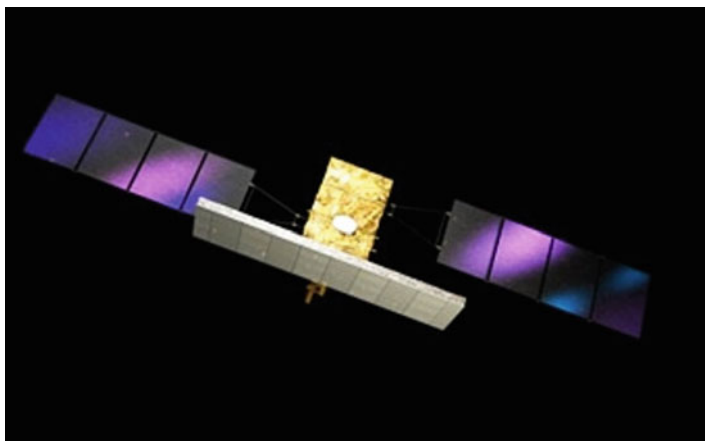
### Earth Observation

Italy has a strong tradition in research technology and development activities, together with robust synergies among scientific community, governmental institutions, and national industries. A high maturity level was reached in different application domains where Italy today plays a key role: one of them is the Earth observation sector.

COSMO-SkyMed is an Earth observation program, funded by the Ministry of Defence and the Ministry of Education, Universities, and Scientific Research. It consists of a constellation of four satellites equipped with high-resolution X-band radar sensors. The system allows operations under any weather or visibility conditions and with very high revisit frequency. The program is dual-use and provides support in the context of international agreements, including Copernicus, the European program for Earth observation.

The constellation was implemented in stages: the first satellite was launched in June 2007, the second in December 2007, the third in October 2008, and the fourth in November 2010. The ground segment is located at the “Piero Fanti” Space Centre, in Fucino (L’Aquila), for the control of the constellation. There are other locations around Italy for the planning and the acquisition, processing, and distribution of satellite data (Fig. 3).

OPTSAT-3000 is a high-resolution optical satellite for imagery, owned by the Ministry of Defence, with a mission life estimated in 7 years. A team from the



**Fig. 3** Cosmo SkyMed artistic view – Credit ASI

SICRAL Defence Control Center, located in Vigna di Valle (Rome), operates and controls the system, launched in 2017 with VEGA launcher from the French Guyana Space Center. The mission planning, acquisition, and processing of data is made in other sites in Italy. The Israel Aerospace Industries, based on inter-governmental agreements, built the satellite. The system is able to interoperate with the second-generation of radar satellites COSMO-SkyMed, planned to launch in the near future. It provides to the Ministry of Defence the capability to integrate optical and radar data generated by the two systems.

### **European Space Infrastructure and Italian Participation**

Italy, as part of the European Union and the European Space Agency, participates in the Copernicus and Sentinel programs. The European Space Agency is developing six families of Sentinel satellite missions, providing high-resolution radar and optical images and according to the needs of Copernicus. The European Commission coordinates and manages the Copernicus program, in order to provide accurate, timely, and easily accessible information of the Earth, including the marine and atmospheric environments.

Italy participates also in the European Galileo program, a collaboration of the European Union with the European Space Agency to ensure technological independence of Europe and to provide international standards for Global Navigation Satellite Systems. At full operational capability, Galileo consists of 30 Medium Earth Orbit satellites and a ground infrastructure consisting of two Galileo Control Center, one in Germany, in Oberpfaffenhofen (Munich), and the other one in Italy, at the “Piero Fanti” Space Centre, in Fucino (L’Aquila).

In 2014, the validation campaign for the early provision of four types of Galileo services was initiated: open service (OS); commercial (CS); public regulated service (PRS); and search and rescue support service (S&RSS). The types of services offered by the Galileo system are distinguished in open or encrypted based on the needs of the end users.

The Italian government ensures political and industrial support for these European programs, in order to reinforce international cooperation and to guarantee capabilities and applications from and in space.

## **Ground Segment**

### **“Piero Fanti” Space Centre – Fucino (L’Aquila)**

The Fucino Space Centre is the largest civil space center in the world with approximately 170 antennas and 250 employees (engineers, specialist technicians, and operational staff). Owned by Telespazio S.p.a., the center is active since 1963.

The main activities carried out are:

- In-orbit satellite control
- Launch and early orbit phase control
- Telemetry, tracking, and command services

- Ground station network services
- Flight dynamics for all types of satellites and orbits
- Telecommunication, television, and multimedia services
- Operational logistics, field, and hosting services (Fig. 4)

### **SICRAL Joint Control Center – Vigna di Valle (Roma)**

The SICRAL Joint Control Center is located in Vigna di Valle, within the Air Force Base “Luigi Bourlot,” near Roma. It is the only control center in Europe operated by military personnel, and the main missions are, according to the North Atlantic Treaty Organization applicable documentation (Air Joint Publication 3.3 B, regarding the Allied joint doctrine for air and space operations):

- C2 Satellite/Space Control (SICRAL e OPTSAT-3000)
- Space Force Enhancement (satellite communication)



**Fig. 4** “Piero Fanti” Space Center, Fucino (L’Aquila) – Credit: Telespazio S.p.a

- Space Situational Awareness (space situational awareness) (Fig. 5)

### **Matera Space Center – Matera**

The Matera Space Center is active since 1994 and is located within the Space Geodesy Center of the Italian space agency (opened in 1983).

It is part of ground station network operated by Telespazio S.p.a. and dedicated to the Earth observation activities. The center acquires, processes, stores, and distributes data from the main remote sensing satellites, and, in addition, produces images, products, and services in near real time for maritime surveillance. The Matera Space Center is one of the three stations of the Core Ground Segment of the European Space Agency, within the Copernicus program.

### **From Upstream to Downstream, Through Midstream**

Italy has a complete chain of products in the space sector. The space economy is the whole chain of value, starting from research, development, and realization of systems (upstream) to the furniture of products and services (downstream). All systems that collect, process, and provide the data and information to the user are called “midstream.”

Since 2016, the Italian Government began to promote a new policy in the space sector based on the signals and activities initiated at European level:



**Fig. 5** SICRAL Joint Control Center, Vigna di Valle (Roma) – Credit: Ministry of Defence



- Scientific and technological programs within the European Space Agency, in collaboration with European Union
- Space program directly funded by the European Union
- The European research and innovation program (Horizon 2020)  
The main programmatic lines were:
  - Institutional funding for research, based on the Italian Space Agency budget, and for Earth observation and telecommunication considering also the Defence funds
  - Technological programs based on funding lines from the Ministry of Economic Development

The space economy is based on the needs provided by the big, medium, and small enterprises in the space and aerospace sectors, in order to provide new services and products based on big data collection and processing capability. At the same time, the Italian Government started to put together all funding lines in space and aerospace sectors, in order to provide a sort of joint funding line (merging the existing ones).

A “strategic plan for space economy” was published in order to provide guidelines and create a National Strategy for Smart Specialization. Six programs started at national level:

- Telecommunication program
- Galileo support program
- Galileo Public Regulated Service infrastructure support program
- Copernicus support program
- Space Surveillance and Tracking support program
- Exploration and space technology development program

---

## Space Security

### Space Security

Space can be considered as the fourth environment of operation, and, therefore, it affects directly national security. Space services and applications – once used only for research purpose – are increasingly entering the everyday life. The services offered by all infrastructures in space will be used more and more by national, regional, and local institutions, as well as by private companies for their business and by citizens to support their daily activities. Furthermore, the use of telecommunication, navigation, and earth observation space capabilities is becoming synergistic with robotics, city management, and drones programs.

The topic of space security is discussed in the world among many national and international for, yet, currently, without a defined and shared definition so far. Usually security is something related to military aspects, not only limited to the services, applications, and exchanged data or information. The demand for space applications is rapidly increasing, due to the awareness of the relevance and

flexibility of space services (like telecommunication, Earth observation, and navigation) in support of everyday life, to operations, and to emergency. At the same time, the quality of services requested by the user is becoming more and more challenging for the industry; therefore, space systems become more complex and harder to manage and control. This leads to the new era of digitalization, artificial intelligence, internet of things, and 5G. Concurrently more countries start to enter in the space and aerospace sectors and markets.

Considering the aforementioned, the number of satellites is increasing, and the technology is rapidly changing. These two aspects are important with respect to the safety and security of space infrastructures and applications.

Therefore, in the last years, the importance of understanding and defining space security is becoming relevant and critical. At the same time, it is strategic to consider the safety of operations in space. Both security and safety in space affect military and civil applications, at national and international level. This means that it is not only a fact of national security. It is also important to take into account the collaboration and cooperation with other nations, interested in ensuring the sustainability of operations in and access to space.

Security, safety, resilience, and sustainability seem to increase their relevance today. How is the relationship between these words? In order to ensure the resilience of space infrastructures and to guarantee the sustainability of space operations, we need to strengthen both the security and the safety of space. The first step is to identify and define what the threats from and in space are.

## Space Threats

It is possible to categorize the space threats in many different ways. One of them takes into account two main groups: intentional and not intentional. The first group is usually related to the security aspects and the second one is more related to the safety. If we consider the intentional threats, they can vary significantly depending on the type of effects they create, the kind of technology they use, and the level of resources needed to develop them. With this in mind, a first classification of threats is possible as below:

- Kinetic physical (counter-space weapons to strike or detonate a warhead)
- Non-kinetic physical (laser, high-powered microwaves, and electromagnetic pulse weapons)
- Electronic (jamming or spoofing radio frequency signals)
- Cyber (attacking the data and not the radio frequency signals)

With respect to the not intentional threats, they are usually related to the natural threats (asteroids, meteors, etc.) or to debris and/or not operational satellites or rocket bodies. We are talking about the so-called environmental safety and monitoring.

At the same time, we can introduce a transversal classification, if we look at the origin of the threats. Therefore, looking at the not intentional threats, we have

ground-based threats (e.g., natural occurrences and power outages), space-based threats (e.g., solar, cosmic radiation, temperature variation, or space objects, like debris or rocket bodies), and interference-based threats (e.g., unintentional human interference). Moving on the intentional threats, we can have sabotage or physical destruction for ground-based, interceptors, or directed-energy weapons for space-based and cyber-attacks or jamming for interference-based.

## Space Surveillance

Italy is one of the main contributors to space in Europe, both in the European Space Agency and in the European Union. The Italian Space Agency has participated in the Space Surveillance and Tracking activities within the European Space Agency program and Italy joined from the beginning the European Commission initiative named Space Surveillance and Tracking Support Framework. The European Union recognized the relevance of space infrastructures and investments, due to the Galileo and Copernicus programs, and decided to begin the Space Surveillance and Tracking initiative with the objective to bring together the Member States' surveillance and processing capacities, in view of setting up an initial European service, consisting of conjunction, reentry, and fragmentation analysis. Since June 2015, Italy is part of the European Union Space Surveillance and Tracking Consortium, together with France, Germany, Spain, and United Kingdom. In 2019, Poland, Portugal, and Romania joined the Consortium.

In particular, Italy has dual-use national space assets both for scientific and operational purposes. Italy recognized the strategic importance of the European Union initiative and decided to join the Consortium, in order to protect national and European access to space and to ensure the safety of operations in space. The Italian Space Agency, the Ministry of Defence, and the National Institute of Astrophysics signed a framework agreement at national level to participate in the European Union Space Surveillance and Tracking Consortium jointly, bringing together resources, knowledge, competences, and capacities in the space surveillance sector.

The Italian Air Force operates the Italian Space surveillance and tracking Operations Center, located at Pratica di Mare Air Force Base, near Roma. The Center uses highly standardized and reliable tools and qualified and skilled personnel to provide:

- Planning and schedule of national sensors
- Processing and evaluation of data and information collected from the sensors
- Exchange of information with the other operation centers (both European and international, like the Combined Space Operations Center in Vandenberg, United States of America)
- Services according to the European Union Space Surveillance and Tracking Service Portfolio (including conjunction, reentry, and fragmentation analysis)

The national sensor's architecture consists of three telescopes (named SPADE, CAS, and PdM-MITE), three radars (named MFDR, BIRALES, and BIRALET),

and one laser (named MLRO). In the near future, the architecture could be extended to other existing or new sensors (either telescopes or radars).

## **Cyber Threats**

The increased interest of governments, companies, and new actors in space leads to the need for a clear understanding of security and cyber issues. It seems that space policy is not yet prepared for the expansion and transformation of space activities, and this leads to growing security risks at national level. It is relevant to understand in a better way what the threats are, also considering the new era of digitalization, strictly connected to the cyber and space domain.

There are simply recommendations for the security and safety of space activities, yet not a regulation or a strategy neither at national nor at international level. We have sensors and processing centers to monitor the situation in space, in order to provide a clear picture of the threats, and, at international level, several initiatives are already in place. Now, the list of threats seems to be clear and updated, but the kind and the type of actions to put in place in order to secure activities and services are probably not so concrete and ready to act.

The number of actors in space is increasing, and the level of threat is rapidly increasing at the same. Therefore, to some extent space is becoming a warfighting domain. Cyber security is facing an increasing level of relevance, and most of the spacefaring nations are discussing, nationally and internationally, how to face the related issues.

Looking at the new digital domain, cyber threats will increase their relevance, and the issue could probably raise its importance, becoming critical for all space infrastructures, both space-based and ground-based.

5G, internet of things, and artificial intelligence are increasing their importance within most of the national and international programs. With this in mind, we need to understand clearly if we are ready to face this new “digitalization era.”

Considering the aforementioned, Italy is currently preparing a National strategy for space security, in view of the relevance of the topic and the need of an international and collaborative approach in this issue.

---

## **Policy, Priorities, and Strategy**

### **New Policy**

According to the Law, the Inter-Ministerial Committee has to define a policy document named “Government Guidelines for the Italian Space and Aerospace Policy.” The President of the Council of Ministers approved the document March 25, 2019.

This document intends to give a general introduction related to the importance of the space and aerospace sectors in Italy and, then, providing the way ahead at

national level in terms of strategy (main pillars as programs and strategy to implement) and activities (prioritized).

This document provides the guidelines for the preparation of two other documents:

- The “Strategic Document on National Space Policy,” to define the political strategy and the lines of financial intervention for the development of innovative industrial technologies and space applications and services in favor of national economic growth
- The “Strategic Vision Document for Space,” to identify strategic goals and objectives for the development of the national space sector

Furthermore, the Coordination Board created a working group with the task to define a National Space Security Strategy, to focus on the protection of space infrastructures from not intentional (e.g., debris or space weather) or intentional threats (e.g., direct actions on ground or in-orbit, electromagnetic interference, and cyber-attacks). Although still being developed, the main contents are related to:

- *Adequate level of continuity of services*  
Reliability, resilience, robustness, and, therefore, continuity of services, as for the Regulated Public Services (Galileo PRS model), in communications (e.g., Govsatcom), and Earth observation (e.g., Copernicus Security Services). In addition, the European Union seems to be moving in the same direction. Italy is supporting the internalization of institutional services (avoiding outsourcing the management to Entrusted Entities), within the EU Space Program Regulation (2021–2027). Security in space cannot be delegated or outsourced, considering its relation to national security.
- *Space safety – natural events/not intentional threats*  
The increased number of satellites corresponds to the increasing in vulnerabilities for all space infrastructures. Low Earth Orbit is starting to be more and more congested. If we look at the new mega-constellation of satellites the number of orbital object could increase drastically and lead to a collapse of all orbits (Kessler Syndrome). At the same time, we can start envisaging the same trend also for Geostationary Orbit. Therefore, it is essential to reduce the risk of in-orbit collisions with an adequate national Space Surveillance and Tracking, integrated with Space Weather. In this regard, a working group, led by the Prime Minister Office, is working to define and implement a shared “programmatic-financial planning,” synergistic with the international initiative for Space Situational Awareness activities at international level.
- *Space security – intentional threats*  
New technologies to enable the so-called in-orbit servicing – “maneuvering satellites,” “co-located satellites,” and “anti-satellite satellites” – lead to the need of an increased space security. Without regulations and agreements in place, it is essential to create a robust infrastructure for monitoring the situation

in space and safeguarding national satellites. In addition to space operations, access to and return from space must be ensured. This will probably lead to the consolidation of Space Traffic Management.

- *Cyber security*

Space security is also related to the intentional threats, including the cyber-attacks or disturbing actions on ground segment, so-called electromagnetic interference. All national space infrastructures shall meet the user needs related to cyber security and electromagnetic interference.

In addition, the Government Guidelines provide indication for the definition of upstream, midstream, and downstream development plans.

The space and aerospace sectors and their capabilities and technologies, through the development and upgrading of applications and operational services will improve the daily life of citizens. Therefore, the institutional user will define the requirements for new systems, applications and space programs focusing on the needs of the user communities.

## **Pillars**

The Inter-Ministerial Committee, with the Government Guidelines for Space and Aerospace Policy, has provided a list of programs and related strategy to implement at national level. The pillars of the Italian strategy are, as per the Government Guidelines document:

- To support of industrial policy and new technological chains, in order to increase the competitiveness at international level
- To strengthen the international cooperation with all international organization in the space and aerospace sectors
- To provide a multiannual planning from both financial and programmatic perspective, in order to provide a clear view of the short-, mid-, and long-term plan for development and realization of space programs
- To reinforce the value of space applications and technologies
- To consolidate a space economy plan in order to support the public-private partnership
- To define a National Space Security Strategy, including the monitoring of objects in space and the mitigation of cyber threats
- To facilitate the access to funds for the small and medium enterprises
- To valorize the national resources
- To support the development of all chains of the space domain. With this in mind, it will define the following:
  - Downstream development plan
  - Midstream development plan
  - Upstream development plan

## Priorities

According to the Law, “The Committee defines the policy directive of the Government in space and aerospace matters, regarding research, innovation, technology and return for the industrial sector, as guidelines for editing the Strategic Document on National Space Policy.” The document is the “Government Guidelines for the Italian Space and Aerospace Policy,” where the national strategic areas for space and aerospace sectors are listed and prioritized:

- Telecommunication, Earth observation and navigation, and services and applications will be used by the community of users, and they need to be promoted by the institutions.
- The study of the universe, through the participation to the international cooperation programs and activities, in particular with European Space Agency and National Aeronautics and Space Administration, also considering the relevance of scientific and technological leadership of Italy at international level.
- Access to space, with reference to the traditional and future concepts, as strategic capability and part of the national industrial sector, in order to foster the commercial exploitation at national and international level.
- Suborbital flights and stratospheric platforms, also considering the development of national spaceport (the first one is Taranto-Grottaglie spaceport).
- In-orbit servicing and de-orbiting, in order to ensure the resilience and the continuity of the operations in-orbit and also the technological applications.
- Robotic exploration of space, related to the moon, the asteroids and other planets, considering the competence of the national scientific and industrial communities, through the development and operation of equipment and experiments onboard the satellites and probes developed within the framework of international collaboration at bilateral and multilateral level.
- Human exploration of space, ensuring and promoting the national excellence in the sector developed in the past years, consolidating the participation in the International Space Station and the new initiatives at international level, such as the exploration of the moon and the developing of new space stations.

## Needs for a Strategy

A National Strategy for Space Security is one of the pillars of the Government Guidelines. Italy recognizes the need of ensuring institutional and commercial users of space an adequate level of resilience from space threats and continuity of services. Intentional or not intentional threats to space-based and ground-based assets are needed to be adequately secured and made safe. Space Surveillance and Tracking, Space Situational Awareness, and, in the future, Space Traffic Management are enablers for the safety and sustainability of space activities. Cyber security is enabler for security and resilience of space infrastructures, both space-based and ground-based.

With this in mind, space diplomacy and international collaboration are two pillars in order to foster a safe and secure space. Bilateral and multilateral approaches to

these issues are the best way to increase the resilience of space infrastructure and the sustainability of space activities. Some initiatives at international level have already started, and, in the near future, they need to be promoted and enhanced.

---

## Conclusions

Italy has a very long history and heritage in the space sector. Beginning in the 1950s, with the development of the first national satellite, the San Marco 1, and its launch, operated by an Italian team, Italy entered into a period of rapid growth for space technologies, applications, and cooperation at international level. Today, Italy is the third contributor of the European Space Agency, and it has, at national level, the knowledge and the experience in the whole chain of supply in space. Earth observation, communication, and navigation are key areas of exploitation and development for all user communities, in order to provide continuity and resilience of services. The increasing numbers of the threats in space, due to the increasing interest of the traditional and the new spacefaring countries, lead to considering strategic the security and the safety of the space domain. With this in mind, the National Law has established an Inter-Ministerial Committee in order to coordinate the space and aerospace activities and policies. The Committee has approved a document named “Government Guidelines for the Italian Space and Aerospace Policy” with the pillars and the priorities in the space and aerospace sectors for Italy. The document provides the guidelines for the preparation of two other documents to be issued within this year: the “Strategic Document on National Space Policy” and the “Strategic Vision Document for Space.” In addition, the Inter-Ministerial Committee will approve a document named “National Strategy for Space Security,” in order to provide the national guidelines for space security and safety.

---

## References

- Defense Intelligence Agency (USA) (2019) Challenges to security in space. Defense Intelligence Agency, Washington, DC
- Delibera del Presidente del Consiglio (25 marzo 2019) Government guidelines on space and aerospace. [http://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/UfficiDiretta\\_CONTE/COMINT/DEL\\_20190325\\_aerospazio-EN.pdf](http://presidenza.governo.it/AmministrazioneTrasparente/Organizzazione/ArticolazioneUffici/UfficiDirettaPresidente/UfficiDiretta_CONTE/COMINT/DEL_20190325_aerospazio-EN.pdf)
- <https://www.cfr.org/report/cybersecurity-and-new-era-space-activities>
- <http://www.telespazio.com/programmes-programmi>
- Legge (7/2018) Misure per il coordinamento della politica spaziale e aerospaziale e disposizioni concernenti l'organizzazione e il funzionamento dell'Agenzia spaziale italiana. <https://www.normattiva.it/uri-res/N2Ls?urn:nir:stato:legge:2018-01-11;7!vig=>
- NATO Standard AJP-3.3 (Ed. B v.1) (2016, April). NATO Standardization Office (NSO) © NATO/OTAN
- Piano Strategico Space Economy (2016) Quadro di posizionamento nazionale Ver. 1.0. [https://www.mise.gov.it/images/stories/documenti/all\\_6\\_Piano\\_Strategico\\_Space\\_Economy\\_master\\_13052016\\_regioni\\_final.pdf](https://www.mise.gov.it/images/stories/documenti/all_6_Piano_Strategico_Space_Economy_master_13052016_regioni_final.pdf)





# British Spacepower: Context, Policies, and Capabilities

# 67

Bleddyn Bowen

## Contents

Introduction .....	1365
Spacepower: Its Time Has Come .....	1367
British Space Policy and Strategy .....	1368
Capabilities .....	1371
Communications .....	1372
SSA .....	1374
ISR/EO .....	1374
Navigation .....	1376
Launch .....	1377
Conclusion .....	1377
References .....	1378

## Abstract

This chapter examines ongoing British military and security space activities in the context of persistent grand strategic problems for the UK. This chapter shows how spacepower is coming of age within the UK, not least in the military dimension. The British state is at something of a crossroads when making choices about its future space development as it has to respond to turbulence across the transatlantic region.

## Introduction

We've got to have this... I don't mind for myself, but I don't want any other Foreign Secretary of this country to be talked at, or to, by the Secretary of State in the United States as I just have with Mr Byrnes. We've got to have this thing over here, whatever it costs. We've

B. Bowen (✉)  
University of Leicester, Leicester, UK  
e-mail: [bb215@leicester.ac.uk](mailto:bb215@leicester.ac.uk)

got to have the bloody Union Jack on top of it. – Ernest Bevin, UK Foreign Secretary, 1946, in reference to atomic bomb technology (Hennessy 2010: 50–51)

In the mid-1940s, Britain had to adapt to its new role as a weakened Empire, dependent on the economic and scientific prowess of the United States, encapsulated by the abrupt exclusion of British scientists and engineers from the American nuclear weapons program shortly after the Second World War. For much of the time since the Second World War, space had been seen as something of an “expensive jolly,” an area where the Americans could expend their wealth and Britain could subsequently capitalize upon through the Five Eyes partnership with minimal financial investment in sovereign British military space capabilities. That old consensus has fractured.

Today, Britain stands at something of a crossroads in its development of spacepower, not least in its military and security elements. Britain is on the cusp of breaking from its past where successive governments never saw much significance to space, and supporters of a greater indigenous military spacepower capability were branded derisively as “space cadets” (SpaceWatch Global 2018). While the British space economy is reaping the benefits of miniaturization of information technology and global data infrastructure, Whitehall continues to grow more interested in space as a wealth generator and source of security and military capabilities in the context of the geopolitical ruptures caused by Brexit and the behavior of the new American president. Indeed, transatlantic security politics continue have repercussions in orbit; space systems and industry do not exist in a geopolitical vacuum. Spacepower is increasingly seen as a form of power any significant actor in the international system must possess, akin to navies, air forces, and nuclear weapons and not just the preserve of the two or three most powerful states in the system. The British state has historically been behind the curve in grasping this geostrategic truth. Since the abandoned attempt at a British missile and rocket capability, Britain has conducted scientific and commercial space activities through the European Space Agency (ESA), the European Union (EU), and private companies, which “removed the need for an autonomous British space program. It took the British government more than thirty years to reach a different conclusion” (Paikowsky 2017: 99). This is typified by the fact that Britain must rely on other states and their resident companies to access this geostrategic environment, as other “middle-powers” have developed their own means of space launch. To use a naval analogy, it would be as if Britain could build ships but would have to contract the Indian state to launch them into the sea. For the first time in its history, the British state has no sovereign means of accessing a vital common and geostrategic environment to its security, prosperity, and influence, in stark contrast to its history with air and sea power. This is not a clarion call for launcher development, rather, it is to show the relative impotence of the UK as a sovereign strategic actor in terms of spacepower – a reality that is often at odds with a British strategic culture more accustomed to a history of imperial dominance through the global commons.

Today, there is a keen effort to put the “bloody Union [Flag]” in space, beyond the highly visible exploits of the astronaut Tim Peake. In 2010, the UK Space Agency

(UKSA) was formed, the *UK Military Space Primer* was published by the UK Ministry of Defence (MoD), and in 2013 and 2017, the Joint Doctrine Publication 0-30 *UK Air and Space Doctrine* was also revised and updated. The year 2014 saw the release of the UK's first National Space Security Policy (NSSP), and in 2015, the first National Space Policy (NSP) was published. At the time of writing, the MoD is in the process of creating the first Defence Space Strategy which is meant to outline space capability gaps across the defense sector that the MoD wishes to fill (MoD 2018a). Spacepower has never enjoyed such sustained attention as a tool of grand strategy and national security in Whitehall as it has in recent years. For the purposes of this chapter, grand strategy is defined as “a purposeful and coherent set of ideas about what a [state] seeks to accomplish in the world, and how it should go about doing so” (Milevski 2016: 140). Grand strategy refers to the way to meet the overarching objectives of a state as articulated by supreme political decision-makers, such as the maintenance of British influence, wealth creation and exploitation, and security within the current form of the international system and its web of alliances. This chapter provides a brief overview of British spacepower from a defense and security perspective. First, it grounds the overview by placing spacepower – which is a cardinal concept for defense and military planners in the twenty-first century – in its British grand strategic context. Second, it provides an overview of the military aspects of British space policy. Third and finally, activities and potential investments in communications, space tracking, remote sensing, navigation, and launchers are summarized.

---

## Spacepower: Its Time Has Come

Spacepower is a concept whose time has come. The 1991 Gulf War was described in some circles as the “First Space War” (Anson and Cummings 1991: 45), because military space systems were instrumental in carrying out battlefield operations and surprise attacks. Since the twilight years of the Cold War, many states have invested in military space applications and have underpinned and enabled their own force modernization programs, resulting the precision-warfare and network-enabled strike forces across Europe and Asia complete with a proliferation in satellite-based command and control, reconnaissance, and navigation systems. With the proliferation of satellites and the growth in the number of space actors throughout the post-Cold War era, spacepower is not only more important for military and economic power, but Earth orbit is also a more target-rich environment. Two decades into the twenty-first century, then, it should be no surprise that three of Earth's most capable military powers continue to develop or have resuscitated weapons program that range from land, sea, and air-launched kinetic-kill satellite interceptors or sophisticated electronic warfare and laser dazzling anti-satellite capabilities (Weeden and Samson 2018).

Spacepower is “the ability of a [state] to exploit the space environment in pursuit of [state] goals and purposes and includes the entire Astronautical capabilities of the [state]. A [state] with such capabilities is termed a space power” (Lupton 1988: 7).

In other words, a space power is an adjective to describe an actor (usually a state) which possesses some form and degree of spacepower, which is a noun or collection of things denoting an ability to use outer space and project influence there. In that sense, spacepower is “just another” tool of grand strategy as one geographic form of power among many (e.g., land, sea, air) made up of several different kinds of thematic forms of power (e.g., military, economic, political, symbolic, scientific) that a state can attempt to marshal for defense and security objectives. Although this chapter focuses on the military and security aspects of British spacepower, they exist in a larger context; military and economic power in their broadest senses are never disconnected in practice as “in the long run one is helpless without the other” (Carr 1974: 132). Alongside sea and air power, spacepower is now a major geostrategic asset and threat for states in the twenty-first century and cannot be ignored. Spacepower produces acute and chronic threats for states, but also short-term and long-term boons through the multitude of military, economic, and industrial applications it enables. After the land, the sea, and the air, space – and Earth orbit in particular – is the fourth geostrategic environment.

---

## British Space Policy and Strategy

The past and present of British spacepower is one of integration and dependence. Britain has integrated with the United States for military and intelligence spacepower, while it has become a significant commercial and scientific spacepower within the European Union (EU) and European Space Agency (ESA) (Bowen 2018a). However, with the incrementally decreasing costs of accessing space, the increasing capabilities afforded to miniaturized computers and more efficient on-board systems, and the growing demand for terrestrial support services and downstream applications, smaller and specialized economies can tap into space development and the exploitation of Earth orbit to a degree that was not possible decades ago. This presents several opportunities for developed economies and middle-power states such as the UK. For decades, the British state has not been pressured to increase its presence in space due to the high level of integration the MoD and intelligence services have enjoyed with the United States under the Five Eyes partnership and the wider “special relationship” which includes the nuclear, space, and missile sectors. However, with American spacepower becoming increasingly taxed in its resources and ability to meet purely American security needs alone, coupled with the increasing benefits of a strong space industrial base, there is an increasing desire for more sovereign UK capabilities in military and intelligence space systems. At present, it is reasonable to portray Britain as a significant second tier space power, sharing its rank with Japan, France, and Germany (Bowen 2018a: 324–330). Britain has clear dependencies in space in many areas – in particular in launch and imagery satellites – but it also has strengths in the commercial sector, research and development, and secure communications.

The publication of the UK’s first space policies, as well as fresh revisions to its spacepower doctrine, reveal a consistent statement of intent on tapping into

spacepower in a more concerted effort than what many in the sector familiar with given the British state's track record in space (Table 1).

Space is arguably not so much of a missing link in British grand strategy and national security policy as it was in the past, if the flurry of official publication activity is any indication. The top-level documents seen here are more educational in their nature, rather than concrete roadmaps for capability acquisition or a shift in de facto policy behavior. Any detail on investments is notoriously hard to pin down, with public statements remaining vague. The documents of most interest here are the 2014 NSSP, the 2015 NSP, the 2017 JDP 0-30, and the embryonic DSS. In the summer of 2018, the DSS was revealed as a document that was still being worked on, and some headline themes for the document were mentioned in conferences and in a leaflet, which are discussed below. The NSSP and NSP recognized space systems as critical national infrastructure and detailed the functions of such infrastructure for the range of government capacities, both civil and military, for the needs of national security (Bowen 2018a: 330–332). This developing ecosystem of documents demonstrates how the British state's organs increasingly recognize spacepower as “just another” source of capability and factor in national security and military power, and that the environment of Earth orbit is just another strategic environment, like the sea and the air. The MoD's space doctrine crystallizes this further by stating in no uncertain terms that:

the military element is only one component of the UK's space power capability, since space is also used to maximise the influence created through diplomatic and economic instruments of national power. A strong commercial space sector, allied space capabilities and civil and scientific expertise are all vital contributors to UK space power. . . UK space power, along with maritime, land, air and cyber power, form the interdependent levers of the military instrument of national power. . . The Space domain should therefore be considered as

**Table 1** Select UK documents relevant to space policy after 2010. Space-specific documents highlighted in gray

Select UK documents relevant to space policy after 2010		
Year	Document	Lead Department/Organization
2010	UK Military Space Primer	Ministry of Defence
2010	National Security Strategy (NSS)	Cabinet Office
2012	Civil Space Strategy, 2012–2016	UK Space Agency
2013	Joint Doctrine Publication (JDP) 0-30, 1st edition	Ministry of Defence
2014	National Space Security Policy (NSSP)	Cabinet Office
2015	National Security Strategy (NSS)	Cabinet Office
2015	National Space Policy (NSP)	UK Space Agency
2017	Joint Doctrine Publication (JDP) 0-30, 2nd edition	Ministry of Defence
2018	Prosperity From Space	Space Growth Partnership
2018	Industrial Strategy	Business, Energy, & Industrial Strategy
2018	Towards a Space Defence Strategy (DSS, leaflet)	Ministry of Defence

routinely as the other operating domains, and must be included in military planning processes. (MoD 2017: 74–75, 117)

Spacepower is being established within the British state's institutions. This ecosystem of documentation and their relations to more generic capstone documents – such as the 2015 NSS – “challenges prevailing notions in the field of space security that ‘space deterrence’ can be considered as a matter separate from and different to deterring war in general” (Bowen 2018a: 330–331). Spacepower is finally emerging from the shadow of nuclear weapons, missile defense, and the “Revolution in Military Affairs” (Gray and Sheldon 1999: 23–25), which has prevented the comprehension of Earth orbit as a co-equal geostrategic environment rather than as a technical component of other terrestrial weapons systems for decades. A hostile act in space will be interpreted and responded to based on political context, strategic effects, and economic costs. The fact that something happens in space does not make it politically unique. The fact that such an act may be in orbit does not condition responses to be more or less violent or escalatory, it depends on the overall strategic context which must take effects, events, and objectives on Earth into account. Space warfare is very much the continuation of Terran politics by other means (Bowen 2019: 556). These are important declaratory moves that challenge persistent and erroneous views throughout society, government, and academia of space activity that space is a realm for scientists and engineers and their experiments alone, or that space is somehow above or beyond terrestrial politics.

This series of space documentation also acknowledges how British freedom of action, sovereignty, or the ability to carry out operations is reliant on allies and the commercial sector. The MoD's space doctrine notes its reliance on American and European allies for key services, not least position, navigation, and timing systems, as well as Earth observation and space-based intelligence capabilities (Bowen 2018a, b). But they remain very general in their description. At the time of writing, the DSS is no more than ministerial statements and a leaflet. At a conference in May 2018, Guto Bebb MP, a former junior minister at the MoD, outlined four general objectives for the DSS: “to enhance the resilience of space systems, to improve operational effectiveness, to enhance space support to frontline troops, and to support wider government activities” (Bowen 2018c). As well as these general themes, the DSS and remarks at the May 2018 conference highlight a desire to develop battlefield-relevant space capabilities, particularly in intelligence, surveillance, and reconnaissance (ISR) support for terrestrial military operations, and increasing the number of space personnel at the MoD from 500 to 600 over the next 5 years (MoD 2018b).

Top-level policy documents such as these often leave “wobble-room” because the practice of grand strategy and the maintenance of national security is often more intuitive, or “an instinctive understanding as to how to handle the instruments of power” (Strachan 2013: 257). When considering British space policy and strategy, it is worth remembering that politics and policy can upend forecasts, long-term commitments, or political priorities and sensitivities at a stroke and change direction faster than any bureaucracy can adapt to on paper. The 2014 NSSP and 2015 NSP

did not foresee the geopolitical rupture of Brexit, which threatens to upend the British space sector's full integration in flagship EU space projects and the EU's space industry (Bowen 2018a: 335–336; Bowen 2018c; Besch 2018; UK House of Commons 2018). It is not the task of such documents to predict the future, but such a massive shift in major geopolitical and macroeconomic position necessitates a radical rethink of the British state's place in the international system.

Yet there are recurring themes that will plague British grand strategy, security policy, and decision-makers as they continue to evolve Britain's defense capabilities and nurture a domestic space industry, no matter how the dust settles on Brexit and President Trump. Richard Aldrich captures this general strategic context well when he argues that:

any venture into space meant tough political as well as technical choices. In the mid-1960s Harold Wilson's cabinet had opted for the British-made Skynet military communication satellite, instead of GCHQ's (Government Communications Headquarters) preferred option of an American-made model. Whether to buy cheap and reliable from the Americans, or to invest in expensive British national capacity (and jobs), or indeed even to join with the Europeans, was a perennial issue. (2010: 438)

These tensions remain, though the EU route for security capabilities will be cut off due to withdrawal from Europe, leaving bilateral options outside EU structure as the only European route for industrial-scale space security asset development. None of the documents above give a clear and consistent idea of which sort of capabilities – beyond encouraging British industry in small satellites – that the MoD and the other organs of state may be interested in developing a sovereign British system or continuing to buy into American system, or integrate with European projects. However, it is not necessarily for those documents to outline a capability program.

---

## Capabilities

When considering existing capabilities and any development and acquisition priorities, it is worth remembering that defense and security cannot be separated from economics, and vice versa. On the international stage, military and economic capabilities and dependencies in space create different forms of influence that shape the governance of outer space and any evolution of legal and security regimes in orbit. Britain is lacking in many government and military satellites with exception to the Skynet military communications satellite system (Bowen 2018a: 325). The UK has no wholly government-owned or military operated Earth observation or ISR satellites, unlike many European states, with exception to some commercial testbed satellites such as the Carbonite-2 live video capture satellite and the NovaSAR small radar satellite. The British commercial space sector has been booming, and is a familiar story to space professionals. At present, the UK space sector employs around 40,000 people, and turnover in the sector has grown from £4.1bn to £13.7bn between 2000 and 2015 (House of Commons 2017: 8–10). The

bulk of the British space sector's income is via space applications (74%), with operations (15%) and manufacturing (8%) trailing far behind in 2015 (UK Space Agency 2016: 6). The success of the British space sector – in particular in commercial communications, small satellite designs and payload manufacturing, and scientific research and innovation – provides a firm footing for British and allied military-industrial complexes to tap into for security and military platforms and personnel, if the political decision was made to expand the UK military and security space sector. Indeed, British-based investors and the UK are a significant source of activity and presence within the start-up space business scene in the global space economy (BryceTech 2018).

If the small satellite research, design, and manufacturing base can survive and maintain its competitive advantages into the 2020s, it places Britain in a decent position to capitalize on the global space economy into the twenty-first century before other states and economic blocs are able to successfully play catch-up and erode Britain's leadership in a niche capability in small satellites and downstream applications. This places Britain in an advantageous position to develop sovereign space security, defense, and intelligence capabilities based on the strengths of its domestic space industrial base. Not unlike the British Empire's maritime past (Kennedy 1976: xv–xvi), Britain's "rise" in military spacepower will only last in the long term if it takes advantage of, and supports in a grand strategic sense, the British state's and society's economic exploitation of outer space. There are many "low-hanging fruit" of military space capabilities that the UK can acquire given its currently small space personnel and hardware footprint, and bring it into parity with its individual European neighbors in terms of sovereign space assets.

Although there is no single British space security program, it is possible to outline British space security and military activities. Britain's difficult position of balancing dependencies is exacerbated on the procurement level by the competing principles of Technology Advantage and Open Procurement. This means that even should Britain decide to acquire, develop, or maintain a capability, there are many technical and practical questions and uncertainties over which specific systems, providers, and operators – domestic or international – are to be pursued to fulfil that capability. Technology Advantage is the MoD's term for the pursuit of defense capabilities on a sovereign basis, those that are to be developed within the UK and to minimize dependence on allies and partners as well as any security liabilities induced by the private sector's modus operandi, regardless of the additional costs of pursuing such capabilities on a unilateral basis and "in-house" at the MoD. Cryptographic and electronic warfare technologies are an example. Open Procurement is the acquisition of defense capabilities through an international competitive tendering process, open to commercial providers from approved international partners (Bowen 2018a: 334–335).

## Communications

The *Skynet* constellation of communications satellites, placed in geostationary orbit, is the longest-lived and arguably most entrenched British military and intelligence



space capability. The system dates back to the 1970s and has enabled secure communications for the British state for decades. Although often seen as an MoD asset, the biggest historical customer of *Skynet* has traditionally been the UK's GCHQ intelligence agency, based in Cheltenham, through the sheer volume of signals intelligence (SIGINT) information they share with the US National Security Agency (NSA) and the limitations and security concerns of pre-fiber transatlantic cables. *Skynet* represented Britain's "first significant step into space" and a concerted effort to maintain some encrypted satellite voice communications capability within Britain by the political leadership, rather than purchasing American equivalents "off the shelf" (Aldrich 2010: 347–348). Today, the *Skynet* system consists of seven satellites, including four *Skynet 5* satellites, and three *Skynet 4* satellites. These satellites provide coverage for most of the globe, apart from the Pacific Ocean. The *Skynet* system provides encrypted high-frequency flexible spot-beam voice communications and data transmission between any terminal at fixed sites and mobile users on land and at sea.

Procurement for the sixth generation of *Skynet* is currently being deliberated in Whitehall, as the new generation is meant to be ready by the early 2020s. There are some concerns over how to build a long-lasting communications satellite given the rapid pace of technological change in communications technology, and may be delaying the decision (Henry 2018). However, the MoD has been consistent in stating that it wishes to bring the operation of *Skynet 6* back in-house, as opposed to the civilian operators of Airbus which has overseen the operation of *Skynet* in recent years. Britain does contain some civilian and commercial expertise in satellite communications, as there are many communications companies registered and based within the UK, not least Inmarsat – a major provider of global maritime satellite communications.

Through the Five Eyes partnership with the United States, the MoD gains significant additional bandwidth for communications. Britain is integrated with the American Advanced Extremely High Frequency (AEHF) and Wideband Global Satcom (WGS) constellations, and *Skynet* is envisioned as part of a system of systems that complements allied communications needs as well as providing a certain degree of sovereign British communications capacity, without having to completely rely on others (Erwin 2018a). Britain's future participation in the EU's GOVSATCOM program is subject to considerable doubt given Brexit and the security protocols in such programs, as well as the cessation of British companies' rights to bid for contracts to develop the future security-relevant hardware and software of *Galileo* due to Britain's decision to rescind its membership of the EU. Given the fact that Britain has continued to invest in this secure communications capability on a sovereign basis and the MoD and Government are increasing their interest in the value of space systems for national security, wealth generation and exploitation, as well as direct British military power, it is not surprising that there is a desire to regain lost skills of satellite operations within the MoD. "Buying British" for *Skynet*, as well as bringing operations in-house to the MoD would help meet the Government's desire to stimulate and support the UK space industry. If the MoD once again oversees the daily operations of its primary satellite program, it will

create a larger corps of space operators and spacepower literacy, as well as a greater demand for the services of the Space Operations Centre (SpOC) at RAF High Wycombe. As far as communications are concerned, British space interests seem to be renewing Technology Advantage and the expense of Open Procurement options.

## **SSA**

Space Situational Awareness (SSA) is another space capability where Britain contributes to allied efforts in building an operational picture of outer space and missile launch detection. Although ostensibly a missile-launch detection and tracking radar, the RAF's Fylingdales radar station in the North Yorkshire Moors can also be used to detect and track space objects, providing more raw data for British and American SSA analysts to identify. Fylingdales also provides atmospheric reentry information relevant to UK territory. However, its primary mission is still for nuclear attack early warning and missile defense for the American system. As such, Fylingdales is not optimized for SSA tasks, but it is still a significant asset in this endeavor. The data from Fylingdales is sent to the United States' Combined Space Operations Centre (CSpOC), where it is compiled with their Space Data Association and the Space Surveillance Network (SSN) and the data from which is then shared back with Britain and provides the data for Joint Forces Command (JFC) and SpOC at RAF High Wycombe, which provides SSA intelligence products to the organs of the British state.

Beyond stating a desire to continue to improve collaboration with America and Europe on SSA data-sharing, as well as signing new memoranda of cooperation with Australia and New Zealand, and SSA-specific multilateral information sharing agreements within the Five Eyes structure (Annett and Dennis 2018: 18), SSA is somewhat muted as a capability for investment from the UK Government. Some argue that it may be best for the British state to provide more freedom for its commercial entities to develop SSA capacities and products (Annett and Dennis 2018: 19, 23). However, as spacepower and Earth orbit becomes more critical for military security and power projection, the need for more sovereign SSA to monitor hostile activities in space may one day encourage Whitehall to support sovereign SSA assets. At present, JFC at the MoD provides the British state with a focal point for SSA assessments and inputs for terrestrial military operations, and is at least an institutional and intellectual basis for the continued development of space operations skills and space intelligence in the UK.

## **ISR/EO**

An area of apparently greater priority is in ISR and EO satellites. Being able to conduct reconnaissance for deployed forces at sea, on land, and in the air would reduce the UK's currently total dependence on allies and commercial providers for

such space-based capabilities. Crucially, such abilities would allow the UK to target imagery assets and acquire sensitive multispectral intelligence in a more focused and secure manner than through using the open market and allies. Specifically, it would help the RAF partially fill a glaring hole in one of its four roles – providing space-based ISR assets and analysis to the “joint” battlefield. At present, neither the RAF nor any other organ of the British state has space-based ISR to call its own. There is a risk that allied space systems may be overwhelmed or otherwise engaged in a crisis or conflict, and such assets may not always be available to the UK on a priority basis from other states. Notably, the MoD and the Defence Science and Technology Laboratory (DSTL) have been a partner in encouraging and developing the Carbonite-2 live video imagery satellite and the NovaSAR small synthetic aperture radar satellite. With some sums of money already invested in these two satellites, it shows how the MoD can contribute to wider industrial strategy goals of nurturing the strengths of British-based space industry, and how the government can become a significant client for the already-successful and sustainable British small satellite sector. Recently, DSTL has advertised a tender worth £750,000 for a feasibility study for a defense-orientated SAR small satellite program, called Project Oberon, with a suggestion that funding for the next phase could be as high as £4 m (Government Online 2018).

Though lacking facilities to rapidly mass produce small satellites at present, stimulating the sector through MoD purchases and requisitions of military variants of small commercial satellites for short-lived or “pop-up” space-based ISR assets for specific battlefield operations could induce greater manufacturing capabilities in Britain. This would also demonstrate a further interest by the MoD of bringing space-based ISR and EO technologies under the “Technology Advantage” umbrella, though the components and supply chains of off-the-shelf technologies will remain a liability. Joint Forces Command (JFC) is the body in the MoD that tasks, requests, and processes ISR support from allies and other providers in space. An MoD equipment plan for 2018–2028 mentions no specific capability investment. However, the “placeholder” is there with a reference to future satellite capabilities (MoD 2018c: 27).

In the American Schriever space wargame of 2018, the UK delegation was given a stronger lead role in commanding the Special Capabilities Integration Cell which “gamed” how the UK, the United States, Canada, and Australia would combine space assets with existing capabilities and potential future capabilities as well (Erwin 2018b). Pop-up small satellite ISR from the British could be a new development to consider in the conduct of future military space operations, particularly as established American ISR infrastructure can be accounted for by potential adversaries in advance of a conflict. Some kind of ISR capabilities for the British state is a feasible goal given that it not only taps into existing strengths in British space industry and would stimulate it further, but it is also relatively affordable. The UK Government invested £21 m in NovaSAR and £4 m in Carbonite-2, with SSTL marketing its range of small satellites in the tens of millions of US dollars. These figures are dwarfed by the UK’s proposed £3-5bn spend on a Galileo replacement UK global navigation satellite system (GNSS).

## Navigation

Despite having supported American attempts to prevent the development of the Galileo satellite navigation system in 2003, in subsequent years, the British space industry became the lead in technology development and manufacturing for Galileo's navigation payload. However, Brexit has upended Britain's privileged position in the development of the Public Regulated Service (PRS) element of the Galileo system. EU regulations, themselves drafted with British input and approval, maintain that only EU member states' industries may win contracts for and develop the security hardware, software, and coding technologies for the PRS. In early spring 2018, the relatively new Secretary of State for Defence, Gavin Williamson, protested at this loss of access to develop PRS components of Galileo for British-based industry as ESA reached decision time on a new round of Galileo procurement. Airbus since 2016 had been planning to move such operations "back into" EU member states as it was cognizant of the EU's space industrial policy and its principle of georeturn to EU member states and security restrictions to non-EU member states.

With much media coverage and ministerial hyperbole, the Galileo system – one few people outside the space sector had previously heard of – had become a household name. The British government has seemingly accepted the figure of £3-5bn for building a replacement GNSS system to sustain the UK's GNSS industrial capabilities and has allocated £92 m for a "feasibility study." Given the costs of SSTL satellites and the UK's investments in technology development ranging in the tens of millions, and UKSA's budget which rests at approximately £375 m per year, 75% of which goes into the common pool at the European Space Agency, these figures for both the proposed British GNSS and the feasibility study are quite large given the supposed capability achieved. Spending approximately one-quarter of the value of UKSA's annual budget on a "feasibility study" for a project that will cost billions over its lifetime to procure and deploy, and many hundreds of millions per annum to operate once deployed, does strike one as more of political theatre rather than serious space capability planning given the daunting opportunity costs imposed by large project in light of other, cheaper, and more acute capability gaps in British military and security space capabilities. This is even more the case when one considers that a British GNSS will triplicate a capability for British MoD. The British will still have access to the secure signals of GPS – of which British industry has never had a part in developing. Meanwhile, the EU has confirmed it would seek to allow the UK passive access to the PRS signal and has already begun considering the application of the United States and Norway to be passive PRS users. Given Britain's value to European security, and that EU rules and statements have only concerned the development of and automatic access to PRS, it is not unrealistic to foresee negotiations in future for Britain to receive passive access to the PRS signal and an ability to manufacture receivers, on the same basis that it does with America's GPS (UK House of Commons 2018). Nevertheless, the future for GNSS expertise in Britain is not certain, as it relied on an EU-funded space program, and the British taxpayer will face a hefty fee if it wishes to keep its Technology Advantage in GNSS capabilities. To maintain it will be an opportunity cost for

British military capability development rivalled perhaps only by the aborted Blue Streak program itself.

## Launch

The opportunity costs of a Galileo replacement system is put into sharper relief when recent British activities in the launch sector are considered. Though the small satellite launch market is rather bleak (Niederstrasser 2018) and not directly militarily relevant as of yet, it is an area of targeted investment from the UK Government. The UK Government is continuing its investment in the British small satellite sector, as well as attempting to develop a UK spaceport for small polar launch vehicles. In 2018, the Space Industry Bill was passed, updating the legislation of 1986 and making it easier to create future space legislation to streamline the oversight and regulation of “NewSpace” or “Space 4.0” actors within the UK. The year 2018 also saw the government attempt to induce commercial small satellite launch providers to develop spaceports in the UK, with London declaring a site on the northern coast of Cataibh (Sutherland) in northern Scotland as its preferred site for vertical polar launches. £50 m in total has been allocated towards developing British spaceport capabilities, with the bulk of the funding allocated towards Lockheed Martin – which owns Rocket Lab, the operators of the Electron launch vehicle – and Orbex, a European small launcher company. What little is left of the £50 m may go to alternative sites such as Tewynblustri (New Quay) in Cornwall which may be a site for Virgin Orbit horizontal launches, and Llanbedr in Gwynedd, near the Eryri (Snowdonia) mountains in Wales, which borders restricted maritime airspace.

A UK-based launch capability based on Open Procurement between American or European owned small launch providers could provide the MoD and the British state with a timelier space launch capability for its pop-up ISR and EO space systems, as well as providing a small launch site closer to home and for European small satellite companies. Such a joined-up capability in terms of sovereign UK small satellite space assets, plus a UK-based space capability, would be transformative for UK space power and the extent to which it could take unilateral actions in high-intensity combat operations on Earth. A sovereign space capability in this sense would go a long way to meeting the UK’s stated grand strategic objectives of being able to conduct and lead military operations where it must. It remains to be seen however whether this future will come about as major investments are needed on both tracks for it to occur, especially in the context of the economic and security tradeoffs between Technology Advantage and Open Procurement.

---

## Conclusion

The UK is at an interesting but turbulent juncture. The UK Government is far more interested than ever before in the military and commercial potential of the so-called “New Space” economy and the UK’s niche strengths in it, while the industry must

deal with the possible disruptions of Brexit, epitomized by the UK's self-imposed exclusion from the continued development of the PRS elements of Galileo as a result of larger political forces. However, Britain's successes in the research and commercial sectors of space place a significant industrial base for the Government to draw upon if it chooses to invest in more capabilities on the ground and in space, and has already crafted the bulk of the necessary top-level documentation that ensures that Whitehall and the Devolved Governments take space security seriously. Battlefield ISR capabilities, hoisted onto small satellites, provide an experimental and relatively affordable pathway for Britain to develop its sovereign ISR space capabilities and reduce its current total dependence on allies.

Whether or not Britain decides to build a replacement GNSS for Galileo and absorb the opportunity costs it presents, the episode has shown that space policy is very much the continuation of Terran politics by other means, and has entrenched the reality of everyday space infrastructure and the military applications of space technology in the minds of a previously ignorant political and media elite, and the general public. However, no matter the scandal or political hubris of the day, British spacepower will always remain caught between the United States and the European Union; the two giants of spacepower on its doorstep. Spacepower has intellectually come of age within Whitehall and is recognized as a tool of grand strategy for any great power in the international system. Britain is starting at a relatively low level of sovereign military and security space capabilities and Britain will have to seek an unfamiliar role in space as it invests more in sovereign assets. This is epitomized by the relationship in access to outer space between Britain and India, where the former imperial possession and postcolonial economy now can provide its former imperial master with the access to outer space that it lacks, for a fee. Given how small the British military space enterprise has been to date, it appears the only way is up for the "bloody Union [Flag]" in space.

---

## References

- Aldrich R (2010) *GCHQ: the uncensored story of Britain's most secret intelligence agency*. Harper Press, London
- Annett I, Dennis R (2018) Increasing resilience in space-based capabilities for the UK through improved space situational awareness and regulatory control. *RUSI J* 163(2):16–26
- Anson P, Cummings D (1991) The first space war: the contribution of satellites to the Gulf War. *RUSI J* 136(4):45–53
- Besch S (2018) A hitchhiker's guide to Galileo and Brexit. Centre for European Reform, 3rd May 2018. <https://www.cer.eu/insights/hitchhikers-guide-galileo-and-brexit>. Accessed 24 Nov 2018
- Bowen BE (2018a) British strategy and outer space: a missing link? *Br J Polit Int Rel* 20(2):323–340
- Bowen BE (2018b) The RAF and space doctrine: a second century, a second space age. *RUSI J* 163(3):58–65
- Bowen BE (2018c) Better the devil you know? Galileo, Brexit, and British defence space strategy. *Defence in Depth*, 23 May 2018. <https://defenceindepth.co/2018/05/23/better-the-devil-you-know-galileo-brexit-and-british-defence-space-strategy/>. Accessed 24 Nov 2018
- Bowen BE (2019) From the sea to outer space: the command of space as the foundation of spacepower theory. *J Strateg Stud*, 42(3–4):532–556

- Bryce Space and Technology (2018) Start-up space: update on investment in commercial space ventures, Alexandria. [https://brycetech.com/downloads/Bryce\\_Start\\_Up\\_Space\\_2018.pdf](https://brycetech.com/downloads/Bryce_Start_Up_Space_2018.pdf). Accessed 02 Dec 2018
- Carr EH (1974) *The twenty years' crisis 1919–1939*. Macmillan, Basingstoke
- Erwin S (2018a) UK MoD still uncertain on how to procure satellite communications. *Space News*, 6th Nov 2018. <https://spacenews.com/u-k-mod-still-undecided-on-how-to-procure-satellite-communications/>. Accessed 24 Nov 2018
- Erwin S (2018b) As satellites become targets, UK military seeks closer ties with space industry. *Space News*, 6th Nov 2018. <https://spacenews.com/as-satellites-become-targets-u-k-military-seeks-closer-ties-with-space-industry/>. Accessed 27 Nov 2018
- Government Online (2018) DSTL Project Oberon contract, 22 November. <http://www.government-online.net/dstl-project-oberon-contract/>. Accessed 22 Dec 2018
- Gray CS, Sheldon JB (1999) Space power and the revolution in military affairs: a glass half full? *Airpower J* 13:23
- Hennessey P (2010) *The secret state: preparing for the worst 1945–2010*. Penguin, London
- Henry C (2018) HTS, megaconstellations feed UK indecisiveness about Skynet 6 program. *Space News*, 7th Nov 2018. <https://spacenews.com/hts-megaconstellations-feed-uk-indecisiveness-about-skynet-6-program/>. Accessed 24 Nov 2018
- House of Commons (2017) Space sector report, London. <https://www.parliament.uk/documents/commons-committees/Exiting-the-European-Union/17-19/Sectoral%20Analyses/34-Space-Report.pdf>. Accessed 2 Nov 2018
- Kennedy P (1976) *The rise and fall of British naval mastery*. Allen Lane, London
- Lupton D (1988) *On space warfare*. Air University Press, Montgomery
- Milewski L (2016) *The evolution of modern grand strategic thought*. Oxford University Press, Oxford
- Niederstrasser C (2018) Small launch vehicles – a 2018 state of the industry survey. In: Paper presented at the 32nd AIAA/USU conference on small satellites. Paper ID: SSC18-IX-01
- Paikowsky D (2017) *The Power of the Space Club*, Cambridge, Cambridge University Press
- SpaceWatch Global (2018) British military space: warfare in space domain part of UK modernising defence programme review. <https://spacewatch.global/2018/12/british-military-space-warfare-in-space-domain-part-of-uk-modernising-defence-programme-review/>. Accessed 22 Dec 2018
- Strachan H (2013) *The direction of war: contemporary strategy in historical perspective*. Cambridge University Press, Cambridge
- UK House of Commons (2018) Exiting the EU select committee, 'Oral evidence: the progress of the UK's negotiations on Eu withdrawal', HC 372, 9th May 2018. <http://data.parliament.uk/WrittenEvidence/CommitteeEvidence.svc/EvidenceDocument/Exiting%20the%20European%20Union/The%20progress%20of%20the%20UK%E2%80%99s%20negotiations%20on%20EU%20withdrawal/oral/82783.pdf>. Accessed 24 Nov 2018
- UK Ministry of Defence MoD (2017) Joint Doctrine Publication 0–30, Shrivenham, Doctrine Development and Concepts Centre
- UK Ministry of Defence (MoD) (2018a) Towards a defence space strategy. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/712376/MOD\\_Pocket\\_Tri-Fold\\_-\\_Defence\\_Space\\_Strategy\\_Headlines.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/712376/MOD_Pocket_Tri-Fold_-_Defence_Space_Strategy_Headlines.pdf). Accessed 4 Nov 2018
- UK Ministry of Defence (MoD) (2018b) UK poised for takeoff on ambitious Defence Space Strategy with personnel boost, 21 May 2018. <https://www.gov.uk/government/news/uk-poised-for-take-off-on-ambitious-defence-space-strategy-with-personnel-boost>. Accessed 24 Nov 2018
- UK Ministry of Defence (MoD) (2018c) The Defence Equipment Plan 2018, 5th Nov 2018. [https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment\\_data/file/753785/20181102-MOD\\_EquipmentPlan2018\\_FINAL-v1.pdf](https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/753785/20181102-MOD_EquipmentPlan2018_FINAL-v1.pdf). Accessed 27 Nov 2018
- UK Space Agency (2016) Summary report: the size and health of the UK Space industry, London, December 2016
- Weeden B, Samson V (2018) *Global counterspace capabilities: an open source assessment*. Secure World Foundation, Washington, DC



Xiaoxi Guo

## Contents

Introduction .....	1382
Satellite Programs Development .....	1383
Earth Observation Satellites .....	1383
Communications and Broadcasting Satellites .....	1387
Navigation and Positioning Satellites .....	1389
Scientific and Technology Test Satellites .....	1391
Future Prospects .....	1395
Earth Observation Satellites .....	1395
Communications and Broadcasting Satellites .....	1396
Navigation and Positioning Satellites .....	1397
Scientific and Technology Test Satellites .....	1397
International Exchanges and Cooperation .....	1397
Conclusions .....	1399
Further Reading .....	1399

## Abstract

The Chinese government considers the space industry as an important part of the nation's overall development strategy. After generations of hard work, China's space industry has created a unique approach of development that conforms to its national conditions, made brilliant achievements symbolized by the successful implementation of several major projects, and obtained a lot of innovative results in space science. Centering on China's satellite programs, this chapter briefly introduces the development history, then outlines specific satellite programs:

---

X. Guo (✉)  
China Academy of Space Technology (CAST), Beijing, China  
e-mail: [vivian\\_gxx@163.com](mailto:vivian_gxx@163.com)



Earth observation, communications and broadcasting, navigation and positioning, and scientific and technological test satellites. Finally, it addresses the satellite program's future perspectives and China's international exchanges and cooperation.

---

## Introduction

Since its establishment in 1956, China's space industry has gradually built up a complete industrial base and has steadily increased its research and development capacity. Currently (as of March 2019), China has the second largest number of spacecrafts in orbit. (Data from the Union of Concerned Scientists, <https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database>.)

The purposes of China's satellite programs are to expand the understanding of the Earth and the universe; to promote human civilization and social progress; to meet the economic demand, technological development, and national security; to raise the scientific and cultural qualities; and to safeguard national interests and enhance comprehensive national power. China has always adhered to the exploration and utilization of outer space for peaceful purposes.

China's satellite engineering was developed on the basis of weak infrastructure industries, relatively underdeveloped scientific and technological level, and limited national funding. Satellite development in China can be divided into three phases.

- *Technology Preparation Phase* (1958–1970). China's satellite development began in the late 1950s. In February 1968, the China Academy of Space Technology (CAST) was established. In April 1970, China launched the first man-made satellite DFH-1, which indicated that China became the world's fifth country to independently develop and launch man-made satellite.
- *Technology Test Phase* (1971–1984). In 1975, China successfully launched and recovered a remote-sensing satellite for the first time. In 1984, China launched the first GEO communications satellite DFH-2.
- *Satellite Application Phase* (1985–Now). On the basis of several successful tests, recoverable satellites and communications satellites were put into practical application. After that, China successfully developed and launched meteorological satellites, communications and broadcasting satellites, navigation and positioning satellites, resources satellites, ocean observation satellites, scientific and technology test satellites.

China unveiled the Belt and Road Initiative (BRI) in 2013, and introduced the Space Silk Road concept in 2014, aiming at creating an entire range of space capabilities including satellites, launch services, and ground infrastructure and at supporting related industries and service providers going global. In this process, China has followed the ancient "silk road spirit" and worked to build a "community with shared future for mankind."

## Satellite Programs Development

China's space industry has witnessed rapid progress manifested by significantly enhanced capacity in independent innovation and access to outer space, constant improvement in space infrastructure, smooth implementation of major projects, and substantial achievements in space science, technology, and applications.

Through continuous efforts, China gradually formed a full range of satellite series, including Earth observation series, communications and broadcasting series, navigation and positioning series, scientific and technology test series. Various satellites have been widely used in many fields, such as society, economy, science and technology, and culture and education.

In recent years, China's commercial space industry has got off to a fast start with the help of microsatellite technologies, and applications such as communications, Earth observation, and technology tests that have been carried out, providing a favorable supplement to China's space system architecture.

## Earth Observation Satellites

China has established a comprehensive system of satellite observation. The performance of the Fengyun (Wind and Cloud), Haiyang (Ocean), Ziyuan (Resources), Gaofen (High Resolution), Yaogan (Remote-Sensing), and Tianhui (Space Mapping) satellite series and the Small Satellite Constellation for Environment and Disaster Monitoring and Forecasting has improved. China's commercial remote sensing satellites are being launched intensively in the last few years.

### Fengyun

The Fengyun polar orbit meteorological satellites have succeeded in networking observation by morning and afternoon satellites, while its geostationary Earth orbit (GEO) meteorological satellites have formed a business mode of "multi-satellites in orbit, coordinated operation, mutual backup and encryption at the appropriate time." So far, China has launched 17 meteorological satellites, eight of which are in orbit, making it the third country after the United States and Russia to have both polar orbit and geostationary meteorological satellites. The Fengyun-4A, the first of China's second-generation GEO meteorological satellites launched in December 2016, has begun serving users in China and across the Asia-Pacific region since May 2018. The Fengyun-4A is enabled with vertical atmospheric sounding and microwave detection capabilities to address 3D remote sensing at geostationary altitudes (Fig. 1).

Apart from the traditional Fengyun series satellites, China also launched a Carbon Dioxide Observation Satellite (TanSat) in December 2016, making China the third country after Japan and the United States to monitor greenhouse gases through its own satellite. The satellite helps understanding climate change and provides China's policy makers with independent data. On a three-year mission, the satellite will thoroughly examine global CO<sub>2</sub> levels every 16 days, accurate to at least 4 ppm (parts per million).



**Fig. 1** Timeline of the Fengyun Series Satellites. (Courtesy of the National Satellite Meteorological Center)

## Haiyang

China operates two families of Haiyang satellites – the Haiyang-1 series and Haiyang-2 series – that carry different sets of oceanography instruments. By the end of 2018, Haiyang-1 A/B/C satellites and Haiyang-2 A/B satellites had been launched, with the capability to observe the ocean dynamic environment. China has basically formed an ocean monitoring capability covering the whole world. As a high-tech means of ocean observation, ocean satellite remote sensing has been widely used in many fields. The latest members of the Haiyang series, Haiyang-1C and Haiyang-2B, were launched in September and October 2018, one after another. Haiyang-2B will replace Haiyang-2A launched in 2011 and will be joined by Haiyang-2C and 2D satellites to form a network around 2020.

## Ziyuan

The Ziyuan-1 02C satellite was launched, the Ziyuan-3 01 and 02 stereo-mapping satellites have achieved double-satellite networking and operating. As China's first civil high-resolution transmission type stereo-mapping satellites, the Ziyuan-3 integrate functions of surveying, mapping, and resources investigation, and acquire high-resolution stereopsis and multispectral images with coverage of the whole nation continuously, steadily, and rapidly for a long time.

## **CHEOS**

In order to improve the comprehensive capabilities of China's Earth observation system, the Chinese government approved to implement China High-resolution Earth Observation System (CHEOS) in 2010, which is established as one of the Major National Science and Technology Projects. The program consists of a fleet of multispectrum imaging and synthetic aperture radar satellites, intended to provide spectral and spatial monitoring that will aid in disaster prevention and reduction, climate, global change monitoring, hydrology, meteorology, and environmental management.

## **Gaofen**

Since the launch of the Gaofen-1 01 satellite in 2013 as part of the country's high-resolution Earth observation project, twelve Gaofen satellites have been launched, six of which were launched in 2018. The Gaofen-5 can detect the state of air pollution in China through observing pollutants, greenhouse gases, and aerosols. It will help reduce the heavy reliance on data on air pollutants and greenhouse gases generated by foreign satellites. The Gaofen-6 satellite has a similar function to the Gaofen-1 satellite but with better cameras, and its high-resolution images can cover a large area of the Earth. Its data will also be applied in monitoring agricultural disasters such as droughts and floods, evaluation of agricultural projects and surveying of forest and wetlands (Table 1).

The system has been combined with other observation means to form all-weather and all-day Earth observation capabilities. By the end of 2018, the Gaofen-1, Gaofen-3 and Gaofen-4 satellites have achieved 100% effective national coverage. Through the implementation of this major project, China has been able to independently acquire all kinds of high-resolution data.

## **Yaogan**

Yaogan series satellites use remote sensing technology and equipment to observe Earth's land cover and natural phenomena, mainly in the fields of territorial resources surveys, environmental monitoring and protection, urban planning, crop yield estimation, disaster prevention and reduction, and space science experiments. Since the Yaogan-1 satellite launched in 2006, China has sent more than 50 Yaogan series satellites into space. The first group of Yaogan-31 and the first group of Yaogan-32 remote sensing satellites were sent into space in April and October 2018 separately.

## **Small Satellite Constellation for Environment and Disaster Monitoring and Forecasting**

The Huanjing-1 A/B/C satellites, members of the Small Satellite Constellation for Environment and Disaster Monitoring and Forecasting have come into service. The final objective of the constellation will consist of four optical satellites and four Synthetic Aperture Radar (SAR) satellites in orbit, to achieve the capability of quantitative, all-weather, all-time disaster forecasting, monitoring, and assessment.

**Table 1** List of On-orbit Gaofen Series Satellites

Satellite	Year Launched	Purpose	Data Distribution (as of the end of 2018)
Gaofen-1 01	2013	China's first Gaofen satellite, a multispectral high-resolution wide-field-imaging Earth observation satellite	9,018,139 views
Gaofen-1 02, 03, 04	2018	Similar to Gaofen-1, but features a smaller bus. China's first civil operational constellation of high-resolution optical satellites, used for land resources investigation, monitoring, supervision, and emergency, etc.	
Gaofen-2	2014	A sub-meter optical land observation satellite	6,869,751 views
Gaofen-3	2016	China's first C-band multipolarized synthetic aperture radar (SAR) imaging satellite with a resolution of 1 m	830,144 views
Gaofen-4	2015	World's first geosynchronous orbit high-resolution Earth observation satellite	463,184 views
Gaofen-5	2018	China's first full-spectrum hyperspectral satellite	
Gaofen-6	2018	China's first satellite capable of performing high-precision agricultural monitoring	
Gaofen-8	2015	Optical remote sensing satellites, mainly used for land survey, urban planning, road network design, agriculture, and disaster relief	
Gaofen-9	2015		
Gaofen-11	2018		

### Commercial Remote Sensing Satellites

Commercial remote sensing satellites, represented by the Jilin-1, Zhuhai-1, and SuperView-1 satellite constellations, are booming. The Jilin-1 satellites are China's first domestically developed commercial Earth imaging satellites. From October 2015 to December 2018, 10 satellites of the Jilin-1 constellation were launched into orbit to provide remote sensing data and product services for government departments and industrial users. Jilin-1 was developed and operated by Chang Guang Satellite Technology Co. Ltd. (also known as CGSTL), belonging to the Changchun Institute of Optics, Fine Mechanics and Physics (CIOMP) under the Chinese Academy of Sciences (CAS). Imagery from the Jilin-1 constellation is offered on the commercial market and is hoped to find application in a number of areas such as forecasting and mitigation of natural disasters, resource exploration and various monitoring tasks (Fig. 2, Table 2).

As of December 2018, seven satellites of the Zhuhai-1 constellation, launched in June 2017 and April 2018, are in orbit to cover the globe every 5 days on average. The Zhuhai-1 is a commercial remote-sensing micro-nano satellite constellation invested in by Zhuhai Orbita Aerospace Science and Technology Co. Upon completion, it will provide satellite big data services for global agriculture, forestry,



**Fig. 2** Gaoxiong, Taiwan Province, China, as seen by the Jilin-1A optical satellite. (Courtesy of Chang Guang Satellite Technology Co. Ltd)

animal husbandry and fishery, water and soil resources, environmental protection, transportation, smart city, modern finance and other industries.

The first phase of the China Aerospace Science and Technology Corporation (CASC) self-developed commercial remote sensing satellite system has been completed. Four SuperView-1 optical satellites, respectively launched in December 2016 and January 2018, are networked as a constellation in orbit with a resolution of 0.5 m, and the revisit period is shortened to 1 day. The SuperView-1 is the first multimeans high-resolution optical remote sensing satellite constellation for commercial use in China. As of December 2018, SuperView-1 had completed global imaging of more than 225,000 views and an area of 24.56 million square kilometers, and its data is being distributed to over 20 countries and regions.

## Communications and Broadcasting Satellites

China has comprehensively advanced the construction of fixed, mobile, and data relay satellite systems. The successful launch of communications satellites such as Yatai (APStar) and Zhongxing (Chinasat) represent the completion of a fixed communications satellite support system whose communications services cover all of China's territory as well as major areas of the world. The Tiantong-1 01 satellite, China's first mobile communications satellite, has been successfully launched. With the Tianlian-1 04 satellite launched in November 2016, the first-generation data relay satellite system composed of four Tianlian-1 satellites has been completed, to provide data relay and control services for China's Shenzhou manned spacecraft, space laboratory and space station missions, as well as other satellites in the low- and medium-Earth orbits.

**Table 2** List of the Jilin-1 Satellites

Satellites	Launch	Imaging modes	Mass	Resolution	Width
Jilin-1 Optical A Satellite	2015/10/7	Push-broom; Large-angle sway	420 kg	0.72 m (panchromatic); 2.88 m (multispectral)	$\geq 11.6$ km
Jilin-1 Smart Video 01/02 Satellite		Staring video	95 kg	1.13 m (color)	4.6 km $\times$ 3.4 km
Jilin-1 Smart Verification Satellite		Push-broom; Staring video; Smart imaging; Stereo imaging	57 kg	4.7 m	9.6 km $\times$ 9.6 km
Jilin-1 Smart Video 03 Satellite	2017/1/9	Staring video; Nighttime light imaging; Stereo imaging; Space object imaging	165 kg	$\leq 0.92$ m (color)	11 km $\times$ 4.5 km
Jilin-1 Video 04/05/06 Satellite	2017/11/21	Staring video; Push-broom; Nighttime light imaging; Stereo imaging; Space object imaging	208 kg	1 m (color)	19 km $\times$ 4.5 km
Jilin-1 Video 07/08 Satellite	2018/1/19	Staring video; Push-broom; Nighttime light imaging; Stereo imaging; Space object imaging	208 kg	$\leq 0.92$ m (color)	19 km $\times$ 4.5 km

Shijian-13 (Chinasat-16) satellite, China's first high-throughput communications satellite that applies electric propulsion technology, was launched in April 2017 and delivered to the customer in-orbit in January 2018. The satellite, built upon the DFH-3B satellite bus, features a Ka-band broadband communications system capable of transmitting 20 gigabytes of data per second, making it the most powerful communications satellite China has developed to date. Shijian-13 represents the development direction of China's communications satellite technology in the next 5–10 years. The integrated electric propulsion, laser communications, advanced electronic system and other technologies will be standard equipment for future communications satellites.

Up to now, the development of China's DFH satellite buses mainly goes through four generations, namely, DFH-2, DFH-3, DFH-4, and the latest DFH-5 satellite buses. The DFH-5 bus incorporates a number of new technologies like high-thrust ion propulsion, a large trussed structure and a much increased payload capacity. The DFH-5 bus is expected to be launched in 2019, leading the upgrade of communications satellites.

Commercial communications satellites developed by China have successfully entered the international market with increasing competitiveness of the associated satellite products. China has exported whole satellites and provided in-orbit delivery of communications satellites to Nigeria, Venezuela, Pakistan, Bolivia, Laos, Belarus, Algeria and other countries. With the successful launch of the APStar-6C satellite in May 2018, China's total number of whole-satellite exported communications satellites reached 10.

The Chang'e-4 relay satellite, named Queqiao ('Magpie Bridge'), is a satellite launched in advance of and in support of China's Chang'e-4 soft landing mission on the Lunar far side. With its launch in May 2018 and insert into orbit in June 2018, Queqiao became the first communication satellite operating in the Halo orbit around the second Earth-Moon Lagrangian (L2) point, to set up a communication link between the Earth and the Chang'e 4 lunar lander.

The two largest Chinese state-owned enterprises and main contractors for the Chinese space program, the China Aerospace Science and Technology Corporation (CASC) and the China Aerospace Science and Industry Corporation (CASIC), are building global low-Earth orbit (LEO) satellite mobile communications and space internet systems, namely the Hongyan Constellation ("鸿雁星座") program and the Hongyun Project ("虹云工程"). In December 2018, the first experimental satellites in the two constellations were launched into space one after another.

The commercialization of high-orbit communication satellites especially high-Earth-orbit high-throughput satellites is moving forward at the same time.

## Navigation and Positioning Satellites

The BeiDou Navigation Satellite System (hereinafter referred to as the BDS) has been independently constructed and operated by China with an eye on the needs of the country's national security and economic and social development. As a space



infrastructure of national significance, the BDS provides all-time, all-weather and high-accuracy positioning, navigation and timing services to global users. China has been laying store by the construction and development of the BDS. It started to explore a path to develop a navigation satellite system suitable for its national conditions since 1980s and gradually formulated a three-step strategy of development.

The BDS is mainly comprised of three segments: space segment, ground segment and user segment. The BDS space segment is a hybrid navigation constellation consisting of Geostationary Earth Orbit (GEO) satellites, Inclined Geosynchronous Satellite Orbit (IGSO) satellites and Medium Earth Orbit (MEO) satellites.

The second-generation BeiDou system (BDS-2) has been offering services to customers in the Asia-Pacific region since December 2012. In 2015, China started building up the third-generation BeiDou system (BDS-3) for global coverage constellation. The first BDS-3 satellite was launched on 30 March 2015. By the end of 2018, the BDS-3 primary system had been completed to provide global services, including countries and regions participating in the Belt and Road Initiative (Silk Road Economic Belt and the twenty-first Century Maritime Silk Road).

Currently (as of the end of 2018), the BDS-1 is already retired. 15 satellites of the BDS-2 are in continuous and stable operation. Before formal deployment of the BDS-3 constellation, 5 BDS-3 test satellites had been launched, to carry out in-orbit test and verification. The BDS-3 satellites equip with the higher-performance rubidium atomic clocks with stability of  $10^{-14}$  and hydrogen atomic clocks with stability of  $10^{-15}$ , which has further improved the performance and lifetime of the satellites. 19 networking satellites (including 18 MEO satellites in operation and 1 GEO satellite under in-orbit test) have been successfully launched, stable and reliable inter-satellite links have been established, and deployment of the core constellation for the BDS-3 has been successfully completed (Fig. 3).

Current basic navigation service performance standards of the BDS are as follows:

- System service coverage: global;
- Positioning accuracy: 10 m horizontally, 10 m vertically (95%);
- Velocity measurement accuracy: 0.2 m/s (95%);
- Timing accuracy: 20 ns (95%);
- System service availability: better than 95%.

In the Asia-Pacific region, the positioning accuracies are 5 m horizontally and 5 m vertically (95%).

The mass applications of the BDS enjoy broad prospects. BDS-based navigation services have been widely adopted by e-commerce enterprises, manufacturers of intelligent mobile terminals and location-based services providers. The services have extensively entered into the fields of mass consumption, share economies, and those related to people's livelihood, which are profoundly changing people's production and livings.



**Fig. 3** China BeiDou Navigation Satellite System. (Image by the BeiDou Navigation Satellite System Website)

### Scientific and Technology Test Satellites

China has developed and launched a series of scientific and technological test satellites, conducted numerous new technology validation tests and space environment exploration missions, and acquired valuable data of space environment, dark matter particles, microgravity, and stereoscopic seismic observation. During the past few years, several “firsts” have been made in the areas of space science and technological test.

#### Shijian Series

China’s Shijian (Practice) satellites test new technologies. Shijian-1 was China’s second satellite and was a platform to test satellite technologies. Shijian-8 was the world’s first satellite devoted to crop breeding. Seeds were placed in the satellite and then exposed to the higher radiation levels of space in the hopes that genetic mutations may occur. The seeds were then removed from the satellite after it returned to Earth and grown. The Shijian-9A satellite, launched in 2012, is a remote sensing satellite with a multispectral imager that took part in the search for Malaysian Airlines flight 370. In 2014, the Shijian-11 program received the first prize in the National Science and Technology Progress Award.

### **Double Star Program**

China has implemented the Double Star Program to explore the Earth's magnetosphere in concert with the Cluster Program of the European Space Agency (ESA), obtaining much new data and making important progress in space physics. Through lunar exploration projects, China has studied the morphology, structure, surface matter composition, microwave properties, and near-moon space environment, further enhancing its knowledge of the moon.

### **Strategic Priority Program on Space Science**

In January 2011, the Chinese Academy of Sciences (CAS) deliberated and approved the implementation plan of Strategic Priority Program on Space Science, signaling its official start. The main goal of the Program is dedicated to deepen the understanding of the universe and planet Earth, seeking new discoveries and new breakthroughs in space science via the implementation of both independent and cooperational space science missions. In November 2017, CAS declared that the four missions making up the Program have been successful. The missions, launched between December 2015 and June 2017, are the dark matter probe "Wukong," the Shijian-10 retrievable satellite, the quantum science satellite "Mozi," and the hard X-ray modulation telescope (HXMT).

### **Dark Matter Particle Explorer (DAMPE)**

China's first space observatory, the Dark Matter Particle Explorer, or DAMPE (also known as Wukong, '悟空' in Chinese), was launched in December 2015. The scientific objectives of DAMPE are as follows: 1) Search for and study of dark matter particles by conducting high-resolution observation of high-energy electron and gamma rays; 2) Study the origin of cosmic rays by observing the high-energy electron and heavy nuclei above TeV; 3) Study the propagation and acceleration mechanism of cosmic rays by observing high-energy gamma rays. There are five payloads onboard the satellite: Si-Pin array, plastic scintillation hodoscope array, BGO calorimeter, neutron detector, and payload data management system. The first results, accurate measurement of electron cosmic-ray energy spectra in space, were published in the international authoritative academic journal *Nature* in 2017. Up to December 2018, DAMPE had been operated for 3 years and reached its expected life span, and 5.5 billion high-energy particles have been detected (Fig. 4).

### **Shijian-10**

China's first microgravity scientific experiment satellite and the 24th recoverable satellite of China, Shijian-10, was launched and then returned in April 2016. The major scientific objectives of Shijian-10 are to get innovative achievements in kinetic properties of matter and rhythm of life by carrying out various scientific experiments in space. Nineteen scientific experiments were carried out onboard the satellite. Among them ten experiments are for microgravity science research, and the other nine experiments are for space life science research.



**Fig. 4** Concept figure of the DAMPE satellite. (Image by the National Space Science Center)

### **Quantum Experiments at Space Scale (QUESS)**

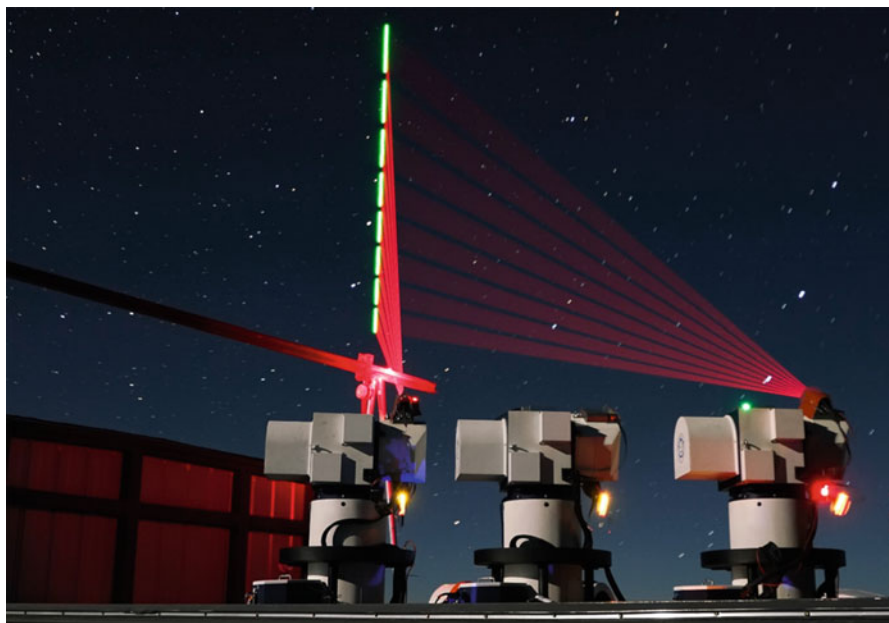
The world's first quantum science satellite, the Quantum Experiments at Space Scale, or QUESS, was launched in August 2016. The satellite is named after the ancient Chinese scientist and philosopher Micius (also known as Mozi, “墨子” in Chinese). QUESS is a proof-of-concept mission designed to facilitate quantum optics experiments over long distances to allow the development of quantum encryption and quantum teleportation technology. As of August 2017, QUESS had accomplished all of its objectives. The QUESS team won the prize delivered by the American Association for the Advancement of Science as it laid the groundwork for ultra-secure communication networks of the future (Fig. 5).

### **Hard X-Ray Modulation Telescope (HXMT)**

Major breakthroughs have been made in space astronomical observation. China's first X-ray astronomy satellite, the Hard X-ray Modulation Telescope or HXMT (also known as Insight, “慧眼” in Chinese), launched in June 2017 to observe black holes, neutron stars, active galactic nuclei, and other phenomena based on their X-ray and gamma-ray emissions. The payloads onboard HXMT include the High Energy X-ray Telescope, the Medium Energy X-ray Telescope, the Low Energy X-ray Telescope, as well as a Space Environment Monitor. Using the direct demodulation method and scanning observations, HXMT can obtain X-ray images with high spatial resolution, while the large detection areas of these telescopes also allow pointed observations with high statistics and high signal to noise ratio. HXMT completed its five-month period of in-orbit calibration and test observations in January 2018, and then officially began science operation.

### **China Seismo-electromagnetic Satellite**

China's first space-based platform for stereoscopic seismic observation system, China Seismo-Electromagnetic Satellite or CSES (also known as Zhangheng-1,



**Fig. 5** This photo, taken on December 10, 2016, shows a satellite-to-Earth link established between QUESS and the quantum teleportation experiment platform in Ali, China's Tibet Autonomous Region. (Image credit: Xinhua)

“张衡一号” in Chinese), was launched in September 2017 to help scientists monitor the electromagnetic field, ionospheric plasma and high-energy particles for an expected mission life of 5 years. Covering the latitude area between  $65^\circ$  north and  $65^\circ$  south, it will focus on Chinese mainland – areas within 1000 km to China's land borders and two major global earthquake belts. CSES has studied several 6–7-magnitude earthquakes of 2018 and found that some disturbances of geomagnetic elements might occur 1–5 days before the earthquake, proving the satellite's reliability and detection capability.

### **Tianyuan-1**

Tianyuan-1, China's first in-orbit refueling system for satellites, was lifted into space by a Long March 7 carrier rocket on June 25, 2016, during the rocket's maiden flight. Tianyuan-1 has conducted nine in-orbit tests including the control and refilling of liquid in microgravity and accurate measurement of propellant, according to the National University of Defense Technology in Changsha, in Hunan province, which developed the system. The spacecraft recorded video and data when it filled three types of propellant tanks. The results of these tests showed Tianyuan-1 has met designers' requirements, the university said, adding that the system features a high level of automation and stability. The recent tests performed by Tianyuan-1 will pave the way for large-scale resupply and refueling for China's future manned space station.

## Future Prospects

In the next period of time China will uphold the concepts of innovative, balanced, green, open and shared development, and promote the comprehensive development of space science, space technology and space applications, so as to contribute more to both serving national development and improving the well-being of mankind.

China plans to expedite the development of its space endeavors by continuing to enhance the basic capacities of its space industry, strengthen research into key and cutting-edge technologies, and implement the BeiDou Navigation Satellite System, high-resolution Earth observation system, and other important projects. Furthermore, the country is launching new key scientific and technological programs, and further conduct research into space science, promoting the integrated development of space science, technology and applications.

## Earth Observation Satellites

In accordance with the policy guideline for developing multifunctional satellites, and creating networks of satellites and integrating them, China will focus on three series of satellites for observing the land, ocean and atmosphere, respectively. China is to develop and launch satellites capable of high-resolution multimode optical observation, L-band differential interferometric synthetic aperture radar imaging, carbon monitoring of the territorial ecosystem, atmospheric Lidar detection, ocean salinity detection, and new-type ocean color observation. China will take steps to build its own capabilities of highly efficient, comprehensive global observation and data acquisition with a rational allocation of low-, medium- and high-spatial resolution technologies, and an optimized combination of multiple observation methods. China will make overall construction and improvement on remote-sensing satellite receiving station networks, calibration and validation fields, data centers, data-sharing platforms and common application supporting platforms to provide remote-sensing satellite data receiving services across the world.

China plans to launch additional nine Fengyun meteorological satellites by 2025, including a number of Fengyun-3 and Fengyun-4 satellites as well as a Sun-synchronous orbit climate-focused satellite and a greenhouse gas detection spacecraft. A total of seven Fengyun-4 satellites are planned to be launched to remain in service through 2037 when a successor program will be inaugurated.

Considering the needs of atmospheric observation by industries and the public on the matter of weather forecasting, atmospheric environmental monitoring, meteorological disaster monitoring and global climate observation, China will continue to improve its large-scale active and passive optical and microwave detection abilities, construct 2 satellite constellations for weather and climate observation, and develop atmosphere detection satellites and hyper-spectrum, laser, polarization observation technologies to detect atmospheric particles, air pollution and greenhouse gas. What's more, China will also intensify satellite data sharing with world meteorological organizations, to form a complete system of atmospheric observation.

In order to meet the great demand in the field of marine resources development and environmental protection, China will develop a variety of optical and microwave observation technologies, construct satellite constellation on marine dynamics and ocean color, develop ocean surveillance satellites, to continuously improve the comprehensive ability of ocean observation. Afterward, China will continue to develop satellites on ocean salinity and marine environmental monitoring, to meet the great demand of marine environmental protection.

Apart from the conventional land observation satellites, China will also develop electromagnetic monitoring satellites, terrestrial carbon monitoring satellites, water cycle observation satellites, and gravity gradient measurement satellites, to monitor the geophysical environment change required by industries specialized on earthquake, disaster prevention and mitigation, and climate change. China aims to foster the monitoring capabilities in geophysics and terrestrial carbon sink to support earthquake prediction and climate change research.

In near future, CASC will develop high-end optical satellites, agile SAR satellites and other commercial satellites to increase the diversity of commercial remote sensing satellites.

Chang Guang Satellite Technology Co., Ltd. plans to complete networking of 60 satellites by 2020 and realize a 30-min revisit to any location on the Earth; complete networking of 138 satellites by 2030 and realize a 10-min revisit to any location on the Earth.

## **Communications and Broadcasting Satellites**

As for the satellite communications broadcasting system, China will continue to operate in a commercial mode and satisfy public welfare needs in the meantime. The main concerns are the development of fixed and mobile communications and broadcasting satellites, and their ground facilities, such as control stations, gateway stations. Through all these efforts, it is expected to provide services of broadband communication, fixed communication, television live broadcasting, mobile communication and mobile multimedia broadcasting, and gradually build satellite communication and broadcasting systems, to be integrated with ground communication networks and covering the world's major regions to facilitate Broadband China Strategy, the globalization strategy and international communication abilities.

As planned, three or four of high-throughput communications satellites will be put into orbit by the latter period of the 13th Five-Year Plan; the Chinasat-18 high-throughput communications satellite will be sent into space in 2019 and its coverage will extend to the entire China in combination with the Chinasat-16; and, two GEO high-throughput satellites with ultra-large capacity will be launched into space roughly in 2023. High-orbit communications satellite can be applied to many areas such as education, marine communications, emergency communications, and outdoor security, and caters for multilayer demands regarding to the Belt and Road Initiative, military–civilian integration, frontier defense, and targeted poverty alleviation.

According to planning, nine Hongyan satellites will be launched by 2020 to test the system, which ultimately will comprise 320 satellites; the Hongyun project will place 156 satellites in orbit. Through these systems, six application services, namely, mobile terminal communication, broadband Internet access, Internet of things, hot spot information push, navigation enhancement, and aviation navigation monitoring, can be provided worldwide, and China's satellite communication coverage will be extended to the ocean and even polar regions for the first time.

## **Navigation and Positioning Satellites**

In the future, the BDS will continue to improve service performance, expand service functions and enhance continuous and stable operation capability. Before the end of 2020, the BDS-2 will launch 1 backup GEO satellite, the BDS-3 will launch another 6 MEO, 3 IGSO and 2 GEO satellites, to further improve global basic navigation and regional short message communication service capabilities, and to achieve the global short message communication, satellite-based augmentation, international search and rescue, and precise point positioning service capabilities. The BDS is planned to provide the following services through various types of satellites in 2020. With the BDS as core, a comprehensive positioning, navigation, and timing (PNT) system will be established and improved before 2035, which will be more ubiquitous, integrated, and intelligent.

## **Scientific and Technology Test Satellites**

In July 2018, the Chinese Academy of Sciences (CAS) officially launched the Strategic Priority Program on Space Science (Phase II). Upon great scientific achievements by Dark Matter Particle Explorer (DAMPE), Quantum Experiments at Space Scale (QUESS), Hard X-Ray Modulation Telescope (HXMT), ShiJian-10 Recoverable Satellite, and so on from Phase I, the program will launch four more space science satellites in the next 5 years. The new patch of space science satellites, includes Einstein Probe (EP), Advanced Space-based Solar Observatory (ASO-S), ESA-CAS Solar Wind Magnetosphere Ionosphere Link Explorer (SMILE), all of which have officially entered its engineering phase. Gravitational Wave High-energy Electromagnetic Counterpart All-sky Monitor (GECAM) is carrying out Phase A study and will enter engineering phase soon.

## **International Exchanges and Cooperation**

The Chinese government holds that all countries in the world have equal rights to peacefully explore, develop and utilize outer space and its celestial bodies, and that all countries' outer space activities should be beneficial to their economic development and social progress, and to the peace, security, survival and development of mankind.



International space cooperation should adhere to the fundamental principles stated in the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space. China maintains that international exchanges and cooperation should be strengthened on the basis of equality and mutual benefit, peaceful utilization and inclusive development.

Over the years, China has exported communications satellites and remote sensing satellites to several countries and regions. At the same time, China has vigorously promoted international cooperation by sharing satellite resources and cooperating in building space and ground infrastructure. As one of the four major GNSS providers, the BDS persists in open cooperation and resource sharing, actively carries out international exchanges and cooperation, and promotes the development of global satellite navigation. BDS-enabled products have been exported to more than 90 countries, providing users with a variety of choices and better application experience.

China and Brazil, through the mechanism of the Space Cooperation Sub-committee of the Sino-Brazilian High-level Coordination Commission, have conducted constant cooperation in the China-Brazil Earth Resources Satellite (CBERS) program. On the basis of the CBERS-4 launched in December 2014 and other satellites, China and the space agencies of Brazil, Russia, India, and South Africa cosponsored and actively promoted cooperation in the BRICS remote-sensing satellite constellation.

Within the mechanism of the Sino-French Joint Commission on Space Cooperation, the China-France Oceanography Satellite (CFOSat) was successfully launched in October 2018. As the first satellite-related cooperation between China and France, the CFOSat is equipped with the world's most advanced technologies. The CFOSat, complementing other existing oceanography satellites, will study the dynamics of waves and how they interact with surface winds, and deepen our understanding of their formation and physical mechanism.

The mission of China Seismo-Electromagnetic Satellite is part of a collaboration program between the China National Space Administration (CNSA) and the Italian Space Agency (ASI), and developed by China Earthquake Administration (CEA) and Italian National Institute for Nuclear Physics (INFN).

China has strengthened bilateral and multilateral cooperation through the Belt and Road Initiative (Silk Road Economic Belt and the twenty-first Century Maritime Silk Road, also known as BRI). Within the BRI, China actively conducts cooperation with other B&R countries in space technology and makes its applications satellite systems and technologies available to them. In terms of satellite navigation, so far, more than 30 B&R countries, including Pakistan, Saudi Arabia, Myanmar and Indonesia, have signed agreements to embed BDS domestically. By the end of 2018, its services had covered all countries and regions participating in the BRI. In terms of satellite remote sensing, the Gaofen-1 and Gaofen-2 have fulfilled their duties as on-duty satellites under the International Charter on Space and Major Disasters in proving important data support to the monitoring and evaluation of floods in Sri Lanka and Bangladesh. Besides, the Fengyun meteorological satellites have gradually covered about 40 B&R countries.

China encourages and endorses the efforts of domestic scientific research institutes, industrial enterprises, institutions of higher learning and social organizations to develop international space exchanges and cooperation in diverse forms and at various levels under the guidance of relevant state policies, laws and regulations.

---

## Conclusions

China is determined to quicken the pace of developing its space industry and actively carry out international space exchanges and cooperation so that achievements in space activities will serve and improve the well-being of mankind in a wider scope, at a deeper level, and with higher standards. Through independent development efforts in developing application satellites and satellite applications, China has made positive contributions to human space exploration. China has also innovation capability in space. It focuses on implementing important strengthening science and technology space projects to realize leapfrog development in space science and technology by way of making new breakthroughs in core technologies and resource integration. China is actively building a space technology innovative system featuring integration of the space industry, academia, and the research community, with space science and technology enterprises and research institutions as the main participants. It has strengthened in the space field and multiple basic research advanced frontier technologies to increase sustainable innovative capacity in space science and technology. No matter the past, present, and future, China advocates peaceful use of space around the world and is willing to cooperate with other countries to develop satellite programs and realize a win-win situation based on the principles of mutual respect, mutual benefit, and equality.

---

## Further Reading

- BeiDou Navigation Satellite System website. <http://en.beidou.gov.cn/>
- China Aerospace Science and Technology Corporation website. <http://english.spacechina.com/n16421/index.html>
- China Daily website. <http://www.chinadaily.com.cn/>
- China National Space Administration website. <http://www.cnsa.gov.cn/english/index.html>
- Chinese Academy of Sciences website. <http://english.cas.cn/>
- Ministry of Foreign Affairs of the People's Republic of China website. [https://www.fmprc.gov.cn/mfa\\_eng/](https://www.fmprc.gov.cn/mfa_eng/)
- National Satellite Meteorological Center website. <http://www.nsmc.org.cn/en/NSMC/Home/Index.html>
- Report on the Development of BeiDou Navigation Satellite System (2018) (Version 3.0), China Satellite Navigation Office, December 2018
- University of Science and Technology of China website. <http://en.ustc.edu.cn/>
- White Paper – China's Space Activities in 2016 The State Council Information Office of the People's Republic of China, December 2016



# Chinese Space Launch Program

# 69

Lehao Long, Lin Shen, Dan Li, Hongbo Li, Dong Zeng, and Shengjun Zhang

## Contents

Introduction .....	1402
Development Background of China's Launch Vehicles .....	1402
Launching Plan and Development of China's Launch Vehicles .....	1403
International Commercial Launch of Long March Launch Vehicles .....	1406
Launch Vehicles in Service .....	1406
LM-2 .....	1406
LM-3 .....	1410
LM-4 .....	1413
New Generation Launch Vehicles .....	1415
LM-5 .....	1415
LM-6 .....	1416
LM-7 .....	1416
LM-11 .....	1416
Prospect of Security Policy .....	1417
China's Space Security Policy .....	1417
Space Debris Mitigation of Long March Launch Vehicles .....	1418
Conclusion .....	1419
References .....	1419

---

L. Long (✉)  
Chinese Academy of Engineering, Beijing, China  
e-mail: [longlh@spacechina.com](mailto:longlh@spacechina.com)

L. Shen · D. Li · H. Li · D. Zeng · S. Zhang  
China Academy of Launch Vehicle Technology (CALT), Beijing, China  
e-mail: [tolinsh@sina.com](mailto:tolinsh@sina.com); [lidan7814@sohu.com](mailto:lidan7814@sohu.com); [lhbspace@sina.com](mailto:lhbspace@sina.com); [est\\_zeng@163.com](mailto:est_zeng@163.com);  
[zhangsj98@sina.com](mailto:zhangsj98@sina.com)

---

**Abstract**

China's development of launch vehicles is sticking to the "self-reliance and independent innovation" path. With more than 50 years' experience, China has successfully developed more than ten models of launch vehicles and managed the transition from research test to flight application and from flight application to industrialization. This chapter provides an overview of China's space launch plan. This chapter mainly presents the development history of China's launch vehicles, launch vehicles in service, the new generation of launch vehicles under development, as well as the efforts made by China in the field of space security.

---

**Introduction**

With an increasing capacity of access to space and driven by launch missions, China's development of launch vehicles is sticking to a path of "self-reliance and independent innovation." With more than 50 years' experience, China has successfully developed more than ten models of launch vehicles and managed the transition from research test to flight application and from flight application to industrialization. It has promoted the development of satellites, satellite applications and technology, as well as manned space technology. China has strongly supported the successful implementation of major projects, namely, the "manned space project" and "lunar exploration project" as representative ones.

China aims for safe, reliable, fast, economic, environment-friendly access to space. China's launch vehicles' development goal in the past, present, and future is to promote space exploration technology development and enhance the progress of human civilization.

This chapter mainly presents the development history of China's launch vehicles, launch vehicles in service, the new generation launch vehicles under development, as well as the efforts made by China in the field of space security.

---

**Development Background of China's Launch Vehicles**

As early as the Song Dynasty (in the eleventh century), China invented black powder rocket, which was in line with the principle of rocket propulsion. It spread to the Arab World and the West in the thirteenth century.

The development of China's present launch vehicles began in the mid-1960s. With long exploration and thorough efforts, China has now successfully developed the Long March 1 (LM-1) series, the Long March 2 (LM-2) series, the Long March 3 (LM-3) series, and the Long March 4 (LM-4) series of launch vehicles and is developing a new generation of launch vehicles. It formed a family of Long March

launch vehicles of more than ten kinds of models. With 40 years development, China's space launch technology has made remarkable achievements. The LM launch vehicles experienced many technological leaps, such as from using conventional propellants to cryogenic propellants, from one-time start of the last stage to multi-start, from tandem configuration to parallel configuration, from one vehicle launching one satellite to launching multi-satellites, and from launching cargos to launching astronauts. Now, they can launch different kinds of satellites and manned spacecraft to different types of low, medium, and high Earth orbits. The launch capacity for low Earth orbit (LEO) and geosynchronous transfer orbit (GTO) is 25 t, and 14 t, respectively. The orbit injection precision reaches leading international level. It can meet the diverse needs of different users. The existing LM launch vehicles have the ability to launch spacecraft to the moon and in the deep space.

On April 24, 1970, China's LM-1 rocket successfully launched the Dongfanghong-1 satellite into low Earth orbit, making China the fifth country in the world that successfully launched its own satellite with its homemade rocket.

In 1999, LM-2F launch vehicle successfully launched the experimental Shenzhou spacecraft and laid a solid foundation for the realization of the strategic goals of China's manned space flight, making China the world's third country of independently developing manned space technology, and further enhanced China's aerospace industry status in the international arena. In October 2003, China's first manned space mission was a success. In June 2012, China successfully accomplished the first manned rendezvous and docking.

In October 2007, LM-3A launch vehicle successfully sent China's first lunar probe satellite "Chang'e-1" into preset orbit, marking China's space industry successfully entered the new field of deep space exploration, Chinese nation's thousands of years' dream of flying to the moon started to become a reality.

Launching artificial Earth satellite, manned spacecraft, and lunar probe are three milestones in the development of China's space industry.

---

## **Launching Plan and Development of China's Launch Vehicles**

Up to June 5, 2019, LM launch vehicles carried out 306 launches, and the launch success rate reached 95%. China finished the first 100 launches in 37 years, the second 100 launches in 7 years, and the third 100 launches in 5 years. With one single model, more than 100 launches of the LM-3A series have been realized. It fully verified the reliability of LM launch vehicles and promoted the industrialization of China's launch vehicles. The launch plan of China's launch vehicles will continue to maintain a high density. It is said that China will complete 110 launches with an annual average about 20 times during "the 13th Five-Year" period.

**Table 1** International commercial launch record of LM launch vehicles (1987–2012)

No.	Payload/SC	Launch vehicle	Customer	Launch date	Remarks
1.	Microgravity test instrument	LM-2C F09	Matra Marconi, France	1987/08/05	Piggyback
2.	Microgravity test instrument	LM-2C F11	Intospace, Germany	1988/08/05	Piggyback
3.	AsiaSat-1	LM-3F07	AsiaSat, HK	1990/04/07	Dedicated
4.	BADR-A/Aussat Dummy payload	LM-2E F01	SUPARCO, Pakistan	1990/07/16	Piggyback
5.	Aussat-B1 Aussat	LM-2E F02	Australia	1992/08/14	Dedicated
6.	Freja	LM-2C F13	SSC, Sweden	1992/10/06	Piggyback
7.	Optus-B2	LM-2E F03	Aussat, Australia	1992/12/21	Dedicated
8.	APSTAR-1	LM-3F09	APT, HK	1994/07/21	Dedicated
9.	Optus-B3	LM-2E F04	Optus, Australia	1994/08/28	Dedicated
10.	APSTAR-II	LM-2E F05	APT, HK	1995/01/26	Dedicated
11.	AsiaSat-2	LM-2E F06 (EPKM)	AsiaSat, HK	1995/11/28	Dedicated
12.	Echo Star-1	LM-2E F07 (EPKM)	EchoStar, USA	1995/12/28	Dedicated
13.	INTELSAT-7A	LM-3B F01	INTELSAT	1996/02/15	Dedicated
14.	APSTAR-1A	LM-3F10	APT, HK	1996/07/03	Dedicated
15.	ChinaSat-7	LM-3F11	ChinaSat, China	1996/08/18	Dedicated
16.	Microgravity test Instrument	LM-2D F03	Marubeni Corp., Japan	1996/10/20	Piggyback
17.	Mabuhay sat	LM-3B F02	Mabuhay, Philippines	1997/08/20	Dedicate
18.	APSTAR-IIR	LM-3B F03	APT, HK	1997/10/17	Dedicated
19.	Iridium	LM-2C/SD F02	Motorola, USA	1997/12/08	Dual
20.	Iridium	LM-2C/SD F03	Motorola, USA	1998/03/26	Dual

(continued)

**Table 1** (continued)

No.	Payload/SC	Launch vehicle	Customer	Launch date	Remarks
21.	Iridium	LM-2C/ SD F04	Motorola, USA	1998/ 05/02	Dual
22.	ChinaStar-1 China	LM-3B F04	Orient, China	1998/ 05/30	Dedicated
23.	SinoSat-1	LM-3B F05	SinoSat, China	1998/ 07/18	Dedicated
24.	Iridium	LM-2C/ SD F05	Motorola, USA	1998/ 08/20	Dual
25.	Iridium	LM-2C/ SD F06	Motorola, USA	1998/ 12/19	Dual
26.	Iridium	LM-2C/ SD F07	Motorola, USA	1999/ 06/12	Dual
27.	CBERS-01	LM- 4F04	INPE, Brazil	1999/ 10/14	Dedicated
28.	SACI	LM- 4F04	INPE, Brazil	1999/ 10/14	Piggyback
29.	CBERS-02	LM- 4F08	INPE, Brazil	2003/ 10/21	Dual
30.	APSTAR-VI	LM-3B F06	APT, HK	2005/ 04/12	Dedicated
31.	NigComSat-1	LM-3B F07	NSRDA, Nigeria	2007/ 05/14	Dedicated
32.	ChinaSat-6B	LM-3B F08	ChinaSat, China	2007/ 07/05	Dedicated
33.	CBERS-02B	LM-3B F09	INPE, Brazil	2007/ 09/19	Dedicated
34.	ChinaSat-9	LM-3B F10	China Sat, China	2008/ 06/09	Dedicated
35.	VeneSat-1	LM-3B F11	Venezuelan Ministry of Science and Technology	2008/ 10/30	Dedicated
36.	PALAPA-D	LM-3B F12	PT Indonesia Tbk	2009/ 08/31	Dedicated
37.	Paksat-1R	LM-3B F15	SUPARCO	2011/ 08/12	Dedicated
38.	W3C	LM-3B F17	Eutelsat	2011/ 10/07	Dedicated
39.	NigComSat-1R	LM-3B F18	NSRDA, Nigeria	2011/ 12/20	Dedicated
40.	APSTAR-VII	LM-3B F19	APT, HK	2012/ 03/31	Dedicated

## International Commercial Launch of Long March Launch Vehicles

Since China officially announced that the LM launch vehicles entered the international commercial launch market in 1985, it has successfully launched various foreign-made satellites into orbit and occupied a place in the international market of commercial satellite launch services.

By the end of 2017, China accomplished 60 commercial launches for foreign customers and domestic customers, including 15 piggyback launch services. China's rising aerospace industry attracts international counterparts' attention with its good market reputation and first-class brand image. In the future, China's aerospace industry will greatly expand internationally; make comprehensive and multilevel cooperation with many foreign clients in the fields of product development, system construction, satellite application, resource sharing, personnel exchanges, and manned space flight; and will actively realize the goal of using space technology to benefit human beings.

---

### Launch Vehicles in Service

#### LM-2

The LM-2 series developed in 1970 are mainly used for LEO missions. Currently, the LM-2 series rockets consist of 7 different launchers (LM-2, LM-2C, LM-2C/CTS1, LM-2C/CTS2, LM-2D, LM-2E, LM-2F). But only five of them are showed in Fig 1. Among them, LM-2 and LM-2E are no longer in use.

#### LM-2C/CTS-1/CTS-2

The LM-2C series have two-stage state and three-stage state, mainly used for launching satellites into LEO, SSO, extremely elliptical orbit (EEO), and GTO. It possesses the capability of launching multi-satellites with one vehicle.

#### LM-2C in Two-Stage State

With total length of 43 m, diameter of 3.35 m, LM-2C launch vehicle is mainly used for launching LEO and SSO satellites. Its launch capacity for 200 km LEO and 600 km SSO is 4.1 t and 1.5 t, respectively.

In August 1987, the LM-2C successfully provided piggyback launch of micro-gravity test instrument for French Matra Marconi Company, marking the beginning of China's international cooperation in aerospace industry.

#### LM-2C in Three-Stage State

LM-2C in three-stage state, namely, LM-2C/CTS, is formed by adding a solid upper stage to the LM-2C. It includes LM-2C/CTS-1 and LM-2C/CTS-2. Its total length is 43 m, and the diameter is 3.35 m. LM-2C/CTS-1 mainly used for launching multi-satellites, and SSO satellites, with 1.9 t launch capacity for 600 km SSO. LM-2C/





**Fig. 1** LM-2 series

CTS-2 mainly used for launching EEO satellites and GTO satellites. The GTO launch capacity (inclination 28\_) is 1.25 t.

Between 1997 and 1999, LM-2C/CTS-1 successfully completed “one launcher two satellites” launch for seven times, sending 14 Iridium satellites (2 dummy satellites and 12 communications satellites) into orbit.

Specifications of LM-2C series			
	First stage	Second stage	Third stage CTS-1/ CTS-2
Maximum diameter of core stage (m)	3.35	3.35	/
Propellant mass (t)	172	54.6	2.62/0.125
Propellant	UDMH/ N2O4	UDMH/N2O4	Solid
Engine	YF-21C	YF-24E	Solid
Engine thrust (kN)	2961.6	741.4 (main) 11.8 × 4 (vernier)	107

(continued)

Specifications of LM-2C series

	First stage	Second stage	Third stage CTS-1/ CTS-2
Engine-specific impulse (N·s/kg)	2556.6	2922.37 (main) 2834.11 (vernier) (vacuum)	10.78
Booster number	/		
Booster diameter (m)	/		
Lift-off mass (t)	242		
Total length (m)	43.027		
Fairing diameter (m)	3.35		
Launch capacity (kg) LEO	4100(two stages)		
SSO	1,500 (two stages), 1,900(600 km SSO)		
GTO	1,250		
Current main mission (orbit)	SSO satellite		
Main launch site	Jiuquan, Taiyuan, Xichang satellite launch center		
Research and development entity	China aerospace science and technology corporation		

## LM-2D

LM-2D is a two-stage conventional liquid launch vehicle, mainly used for LEO and SSO missions. It has the capabilities of launching two satellites in parallel and launching multi-satellite with one vehicle.

With total length of 41.056 m and diameter of 3.35 m, LM-2D launch vehicle is mainly used for launching satellites to LEO and SSO. Its launch capacity for 260 km LEO and 600 km SSO is 3.6 t and 1.5 t, respectively.

Specifications of LM-2C series

	First stage	Second stage
Maximum diameter of core stage (m)	3.35	3.35
Propellant mass (t)	124	59
Propellant	UDMH/N <sub>2</sub> O <sub>4</sub>	UDMH/N <sub>2</sub> O <sub>4</sub>
Engine	YF-21C	YF-24C
Engine thrust (kN)	2961.6	742.04 (main) 47.1 (vernier)
Engine-specific impulse (N·s/kg)	2556.6	2,942 (main) 2,834 (vernier) (vacuum)
Booster number	/	
Booster diameter (m)	/	
Lift-off mass (t)	250	
Total length (m)	41.056	
Fairing diameter (m)	3.35	

(continued)

Specifications of LM-2C series		
	First stage	Second stage
Launch capacity (kg) LEO	3,600 (260 km LEO)	
SSO	1,500(600 km SSO)	
Current main mission (orbit)	SSO satellite	
Main launch site	Jiuquan satellite launch center	
Research and development entity	China aerospace science and technology corporation	

## LM-2F

LM-2F is a highly reliable and safe launch vehicle developed to meet the demands of China's manned space special project. LM-2F has two variants of launching Shenzhou spacecraft and target spacecraft. As for launching Shenzhou spacecraft, its diameter is 3.35 m, and total length is 58.3 m. It consists of four liquid boosters, first stage, second stage, fairing, and the escape tower. Its launch capacity for LEO is 8.1 t.

On October 15, 2003, LM-2F successfully sent China's astronaut Yang Liwei into space, making China the third country in the world having manned space capability and also marking China's Manned Space Project entering into a substantive application stage.

Specifications of LM-2F			
	First stage	Second stage	Booster
Maximum diameter of core stage (m)	3.35	3.35	2.25
Propellant mass (t)	184	83.727	45.277
Propellant	UDMH/ N2O4	UDMH/N2O4	UDMH/ N2O4
Engine	YF-20 K	YF-24 K	YF-25 K
Engine thrust (kN)	2961.6	741.4 (main) 11.8 × 4 (vernier)	740.4
Engine-specific impulse (N·s/kg)	2556.6	2922.37 (main) 2834.11 (vernier) (vacuum)	2550
Booster number	4		
Booster diameter (m)	2.25		
Lift-off mass (t)	493		
Total length (m)	58.3		
Fairing diameter (m)	3.35		
Launch capacity (kg) LEO	8,100		
Current main mission (orbit)	LEO		
Main launch site	Jiuquan satellite launch center		
Research and development entity	China aerospace science and technology corporation		

## LM-3

The LM-3 series are made up of four launch vehicles (see Fig. 2), i.e., LM-3, LM-3A, LM-3B, and LM-3C. As LM-3 has been retired, the rest of the three kinds of rockets are known as the LM-3A series of launch vehicles.

### LM-3A

LM-3A is a three-stage liquid launch vehicle, consisting of the first stage, second stage, third stage, and fairing. Its total length is 52.52 m, the diameter of the first stage and the second stage is 3.35 m, and the diameter of the third stage is 3 m. Its standard launch capacity to GTO is 2.6 t.



**Fig. 2** LM-3 series of launch vehicles

Specifications of LM-3A

	First stage	Second stage	Third stage
Maximum diameter of core stage (m)	3.35	3.35	3
Propellant mass (t)	171.843	33.207	18.518
Propellant	UDMH/N2O4	UDMH/N2O4	LH2/LOX
Engine	YF-21C	YF-24E	YF-75
Engine thrust (kN)	2961.6	741.4 (main) 11.8 × 4 (vernier)	82.76
Engine-specific impulse (N·s/kg)	2556.6	2922.37 (main) 2834.11 (vernier) (vacuum)	4,300
Booster number	0		
Booster diameter (m)	/		
Lift-off mass (t)	243		
Total length (m)	52.52		
Fairing diameter (m)	3.35		
Launch capacity (kg) LEO	–		
SSO	–		
GTO	2600		
Current main mission (orbit)	GTO		
Main launch site	Xichang satellite launch center		
Research and development entity	China aerospace science and technology corporation		

### LM-3B

LM-3B is a three-stage liquid launch vehicle employing enhanced LM-3A as the core stage and strapped with four liquid boosters. Its total length is 54.84 m. The diameter of booster is 2.25 m. The diameter of the first stage and the second stage is 3.35 m, and the diameter of the third stage is 3.0 m. At present, LM-3B rocket consists of three variants. Its standard launch capacity to GTO is between 5.1 and 5.6 t.

LM-3B is the main launch vehicle to undertake the high orbit international commercial satellite launching services. It is also the launcher of lunar probe “Chang’e III” and “Chang’e IV.”

Specifications of LM-3B

	First stage	Second stage	Third stage	Booster
Maximum diameter of core stage (m)	3.35	3.35	3	2.25
Propellant mass (t)	171.843	49.876	18.324	37.756
Propellant	UDMH/N2O4	UDMH/N2O4	LH2/LOX	UDMH/N2O4

(continued)

Specifications of LM-3B				
	First stage	Second stage	Third stage	Booster
Engine	YF-21C	YF-24E	YF-75	YF-25
Engine thrust (kN)	2961.6	741.4 (main) 11.8 × 4 (vernier)	82.76	740.4
Engine-specific impulse (N·s/kg)	2556.6	2922.37 (main) 2834.11 (vernier) (vacuum)	4,300	2556.6
Booster number	4			
Booster diameter (m)	2.25			
Lift-off mass (t)	427			
Total length (m)	54.84			
Fairing diameter (m)	4.2			
Launch capacity (kg) LEO	–			
SSO	–			
GTO	5600			
Current main mission (orbit)	GTO			
Main launch site	Xichang satellite launch center			
Research and development entity	China aerospace science and technology corporation			

### LM-3C

LM-3C takes LM-3A as the core stage and is strapped with two liquid boosters at the first stage. Its total length is 54.84 m. The diameter of the booster is 2.25 m, the diameter of the first stage and second stage is 3.35 m, and the diameter of the third stage is 3.0 m. The GTO launch capacity of LM-3C reaches 3.8 t.

Specifications of LM-3C				
	First stage	Second stage	Third stage	Booster
Maximum diameter of core stage (m)	3.35	3.35	3	2.25
Propellant mass (t)	171.843	49.876	18.324	37.756
Propellant	UDMH/ N2O4	UDMH/N2O4	LH2/ LOX	UDMH/ N2O4
Engine	YF-21C	YF-24E	YF-75	YF-25
Engine thrust (kN)	2961.6	741.4 (main) 11.8 × 4 (vernier)	82.76	740.4
Engine-specific impulse (N·s/kg)	2556.6	2922.37 (main) 2834.11 (vernier) (vacuum)	4,300	2556.6
Booster number	2			
Booster diameter (m)	2.25			
Lift-off mass (t)	343			
Total length (m)	54.84			

(continued)

Specifications of LM-3C				
	First stage	Second stage	Third stage	Booster
Fairing diameter (m)	4			
Launch capacity (kg) LEO	–			
SSO	–			
GTO	3800			
Current main mission (orbit)	GTO			
Main launch site	Xichang satellite launch center			
Research and development entity	China aerospace science and technology corporation			

## LM-4

The LM-4 series are made up of three launch vehicles (see Fig. 3), i.e., LM-4A, LM-4B, and LM-4C. As LM-4A has been retired, the rest of the two kinds of rockets are known as the LM-4 series.

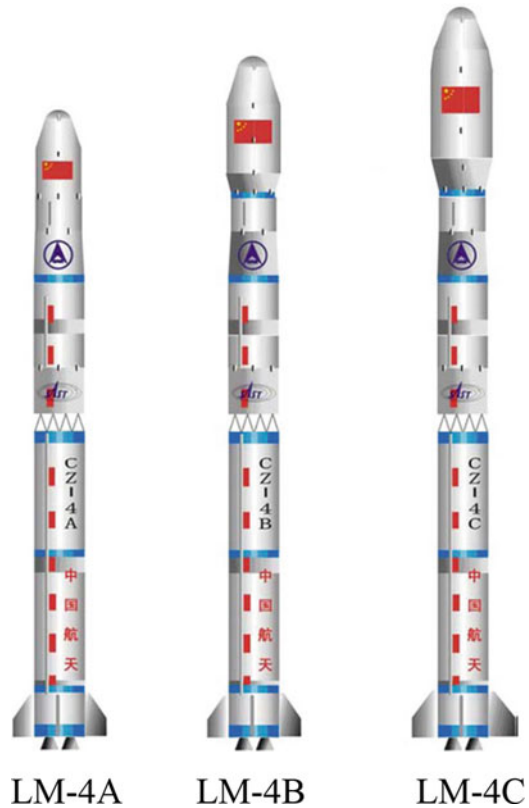
### LM-4B

LM-4B is a three-stage launch vehicle using room-temperature liquid propellants. It is made up of the first stage, second stage, third stage, and fairing. It consists of the vehicle structure, engine, pressurized feeding system, control, telemetry, and external measuring safety subsystems. Its total length is 45.776 m, the diameter of the first and second stage is 3.35 m, and the diameter of the third stage is 2.9 m. LM-4B can implement a variety of orbit missions (SSO, LEO, GTO) and different types of satellite launches. Its launch capacity for 200 km 60° inclination circular orbit is about 4.6 t, and for 400 km sun-synchronous orbit is about 3.2 t. LM-4B is mainly used to send satellites to SSO.

Specifications of LM-4B			
	First stage	Second stage	Third stage
Maximum diameter of core stage (m)	3.35	3.35	2.9
Propellant mass (t)	181.89	35.408	14.34
Propellant	UDMH/ N2O4	UDMH/N2O4	UDMH/ N2O4
Engine	YF-21C	YF-24H	YF-40B
Engine thrust (kN)	2961.6	742.04(main) 46.09 (vernier)	100.848
Engine-specific impulse (N·s/kg)	2556.6	2942.4(main) 2761.6(vernier)(vacuum)	2,971
Lift-off mass (t)	250		
Total length (m)	45.776		
Fairing diameter (m)	3.35		

(continued)

**Fig. 3** LM-4 series of launch vehicles



#### Specifications of LM-4B

	First stage	Second stage	Third stage
Launch capacity (kg) LEO	4600		
SSO/400 km	3200		
GTO	/		
Current main mission (orbit)	SSO		
Main launch site	Taiyuan satellite launch center		
Research and development entity	China aerospace science and technology corporation		

#### LM-4C

LM-4C is an enhanced three-stage liquid launch vehicle by adding new technologies such as restart of the third-stage engine to LM-4B. Its total length is 45.776 m, the diameter of the first and second stage is 3.35 m, and the diameter of the third stage is 2.9 m. Its launch capacity for 600 km trajectory tilted by 60 degree to the equator is about 3.7 t, for 800 km SSO is 2.7 t, and for GTO is about 1.3 t. LM-4C is mainly used to send satellites to SSO.



Specifications of LM-4C			
	First stage	Second stage	Third stage
Maximum diameter of core stage (m)	3.35	3.35	2.9
Propellant mass (t)	189.841	34.449	13.971
Propellant	UDMH/ N2O4	UDMH/N2O4	UDMH/ N2O4
Engine	YF-21C	YF-24H	YF-40A
Engine thrust (kN)	2961.6	742.04 (main) 46.09 (vernier)	100.848
Engine-specific impulse (N·s/kg)	2556.6	2942.4 (main) 2761.6 (vernier)(vacuum)	2,971
Lift-off mass (t)	250		
Total length (m)	47.977		
Fairing diameter (m)	3.8		
Launch capacity (kg) LEO	/		
SSO/800 km	2700		
GTO	1300		
Current main mission (orbit)	SSO		
Main launch site	Taiyuan satellite launch center		
Research and development entity	China aerospace science and technology corporation		

## New Generation Launch Vehicles

China is continuously strengthening the construction of space transportation systems, further perfecting the completeness of LM launch vehicles, enhancing the ability of access to space, and developing a new generation of launch vehicles and upper stages with the LM-5, LM-6, LM-7, LM-11 as the representatives. LM-5 uses nontoxic environment-friendly propellants with LEO launch capacity of 25 t and GTO capability of 14 t. LM-6 is a new and fast responsive rocket, with launch capacity for 700 km SSO not less than 1 t. Launch capacity of LM-7 for LEO and 700 km SSO is 13.5 t and 5.5 t, respectively.

### LM-5

LM-5 is a new large rocket developed under the guideline of “one series, two engines, and three modules.” The “three modules” refers to the 5 m diameter module using liquid hydrogen and liquid oxygen as propellants, the 3.35 m diameter and 2.25 m diameter modules using liquid oxygen and kerosene propellants. The “two engines” refers to the newly developed liquid oxygen and liquid hydrogen engine of 50 t class thrust and the liquid oxygen and kerosene engine of 120 t class thrust. Based on the design concept of “generalization, serialization, and combination,”

six configurations with 5 m-diameter core stage will be formed based on the three newly developed modules. Its GTO launch capacity covers from 6 t to 14 t, and LEO launch capacity from 10 t to 25 t. LM-5 configuration for the first flight is the one strapped with four 3.35 m-diameter boosters.

LM-5 uses brand new power system, large vehicle structural design and manufacturing technology, advanced control, and digital technology, which significantly improve the overall level of China's launch vehicles and the capacity of utilizing space resources. Its total length is 57 m. The diameter of the first stage and second stage is 5 m. The diameter of four strap-on booster is 3.35 m. Its maximum GTO launch capacity is 14 t. The maiden flight of LM-5 took place in November 2016.

### **LM-6**

As a member of the new generation rockets, LM-6 is a light and fast responsive liquid launch vehicle. To meet easy and quick launch requirements, it is transported to the simplified launch pad (without tower) by the self-moving vertical car, then is erected, filled up, and launched. It is 29.9 m long and 3.35 m in diameter. Its lift-off mass is about 102 t, and lift-off thrust reaches about 1200 kN. It adopts three-stage configuration and uses nontoxic propellants such as liquid oxygen and kerosene. With monitoring and control limits, its launch capacity for 700 km SSO is approximately 500 kg. Without considering limits of monitoring and control conditions, its launch capacity for 700 km SSO is about 1,000 kg by means of gliding and restarting of the third stage. The maiden flight took place in September 2015.

### **LM-7**

LM-7 is a new medium-sized launch vehicle, mainly used for launching cargo ship to the space station. Its total length is 53.1 m. Lift-off mass is about 595 t. Lift-off thrust is 735 t. The diameter of the core stage is 3.35 m, and the diameter of the four strap-on boosters is 2.25 m. The maximum launch capacity for LEO is 13.5 t. The maiden flight took place in June 2016.

### **LM-11**

LM-11 is a four-stage solid launcher developed by china aerospace science and technology corporation. It is a quick response and low-cost launcher. The total length of LM-11 is 20.8 m, the maximum diameter is 2 m, the lift-off mass is 58 t, and the lift-off thrust is 120 t. LM-11's capacity of SSO at the altitude of 700 km is 400 kg, the capacity of LEO is 700 kg. The maiden flight of LM-11 took place in Sept 2015. The first sea launch of LM-11 was completed in June 2019.

## **Prospect of Security Policy**

### **China's Space Security Policy**

Outer space is the common wealth of human being, and the exploration of outer space is the unremitting pursuit of mankind. At present, the world space activities are booming. Major space nations successively develop or adjust the space development strategy, development plan and development objectives, status and role of the aerospace industry in the country's overall development strategy have become increasingly important. The impact of space activities on human civilization and social progress has been enhanced.

China puts the development of space industry as an important part of the country's overall development strategy and always adheres to the policy of exploring and using outer space for peaceful purposes. In recent years, China's space industry develops rapidly with some important technology areas having reached the world's leading level. Space activities play an increasingly important role in China's economic construction and social development.

In the future, China will focus on the national strategic goals, strengthen independent innovation, expand opening up and cooperation, and promote sound and rapid development of space industry. Meanwhile, China is willing to work together with the international community to jointly safeguard a peaceful and clean outer space and make new contributions to promote the human peace and development.

China's aims of developing space activities are as follows: to explore the outer space and enhance the understanding of the Earth and the universe; to peacefully use the outer space and promote human civilization and social progress for the benefit of all human beings; to meet the needs of economic construction, scientific and technological development, national security, and social progress; to improve the scientific and cultural quality of human beings; to safeguard national interests; and to enhance overall national strength.

The principle of China's space security policy is subordinate to and serves the overall national development strategy and adheres to the scientific planning, self-development, the peaceful use, and open cooperation principles.

Scientific planning is defined as respecting science and law and comprehensively balancing and scientifically developing space technology, space application, space science, and other space activities based on the development reality of the aerospace industry, to maintain the comprehensive, coordinated, and sustainable development of aerospace industry.

The meaning of self-development always adheres to the independent and self-reliant path of development, which mainly relies on our own power to self-develop the space industry according to national conditions and national strength, to meet the basic needs of the country's modernization drive.

Peaceful use means always adhere to the peaceful use of outer space, opposes weaponization of outer space and arms race in outer space, rationally develops and utilizes space resources, and effectively protects the space environment, letting space activities bring benefits to the people.

Open cooperation refers to adhere to the combination of being independent and cooperating openly, on the basis of equality and mutual benefit, peaceful utilization and common development, actively carrying out international exchanges and cooperation in the space industry, and committed to the common progress of human space industry. International cooperation in the space field should follow the basic principles of United Nations' *Declaration on International Cooperation in the Exploration and Use of Outer Space for the Benefit and in the Interest of All States, Taking into Particular Account the Needs of Developing Countries*.

In the next 5 years, China will strengthen the basic capacity building of aerospace industry, advance the deployment of cutting-edge research, and continue to implement major scientific and technological projects and priority projects in key areas, such as the manned spaceflight, lunar exploration, high-resolution Earth observation system, satellite navigation and positioning system, and the new generation of launch vehicles. It will comprehensively improve space infrastructure, promote the development of satellite industry and its application industry, conduct space science research in depth, and enhance the comprehensive, coordinated, and sustainable development of the aerospace industry.

## **Space Debris Mitigation of Long March Launch Vehicles**

Established in 1993, the Inter-Agency Space Debris Coordination Committee (IADC) aims to strengthen the research and coordination of member states in the field of space debris. China is also a member of the committee. As a space power, China actively participates in the related anti-space debris activities and conscientiously fulfills the duties and obligations that it commits to IADC, in order to protect the image and status of China's aerospace industry in the international arena.

China organizes experts in the fields of aerospace and space policy to study the feasibility of the design and management of space debris mitigation and formulated the Guideline for Orbital Debris Mitigation in 2006. From technical aspects, the standard puts forward basic requirements on the design of orbital debris in each step of space activities. Those basic requirements are consistent with IADC's guidelines for space debris mitigation. Based on the Guideline for Orbital Debris Mitigation, China is gradually setting design and management standards for space debris mitigation.

In accordance with international conventions, China will greatly promote the space debris mitigation design of Long March launch vehicles. For LEO missions, life of the last stage in orbit is less than 25 years, and passivation measures are generally adopted; for SSO missions, active de-orbit measures or passivation measures are taken.

In the future, China will continue to strengthen the space debris monitoring, mitigation and spacecraft protection in the field of space debris. It will develop space debris monitoring and collision warning technology and carry out the monitoring and collision warning of space debris and small near-Earth celestial bodies. It will establish evaluation system of space debris mitigation design and actively take space

debris mitigation measures on the after-mission spacecraft and launch vehicles. It will test digital simulation technology of space debris impact and promote the construction of space debris protection system.

---

## Conclusion

Free exploration, development and utilization of outer space and celestial bodies, is the equal right shared by countries in the world. Each country's outer space activities should contribute to its national economic development and social progress and should benefit human security, survival, and development. China's launch vehicle technology development will contribute to the technological progress of world's space exploration. China advocates strengthening international exchange and cooperation and promoting inclusive development in the space industry on the basis of equality and mutual benefit, peaceful use, and common development.

---

## References

- China Academy of Launch Vehicle Technology, website: <http://calt.spacechina.com/n482/n498/index.html>
- China Aerospace Science and Technology Corporation, website: <http://www.spacechina.com/n25/n146/n238/n12985/index.html>
- China's Space Activities (2011), China National space Administration website, <http://www.cnsa.gov.cn/n6758824/index.html>
- China's Space Activities (2016), China government website: [http://www.gov.cn/xinwen/2016-12/27/content\\_5153378.htm](http://www.gov.cn/xinwen/2016-12/27/content_5153378.htm); China National space Administration website: <http://www.cnsa.gov.cn/n6758824/index.html>



# Indian Space Program: Evolution, Dimensions, and Initiatives

# 70

Hanamantray Baluragi and Byrana Nagappa Suresh

## Contents

Introduction .....	1422
Evolution of the Indian Space Program .....	1423
Initiation Phase (1960–1970s) .....	1423
Experimental Phase (1980s) .....	1424
Operational Phase (1990s) .....	1425
Expansion Phase (2000s) .....	1425
Dimensions of the Indian Space Program .....	1426
Space Applications .....	1426
Space Infrastructure .....	1428
Space Transportation System .....	1430
The Human Spaceflight Program: A New Beginning in the Indian Space Program .....	1433
New Initiatives Toward Low-Cost Access to Space .....	1435
Small Satellite Launch Vehicle .....	1435
Reusable Launch Vehicle: Technology Demonstrations .....	1436
Hypersonic Air-Breathing Engine .....	1438
Conclusion .....	1439
References .....	1439

## Abstract

With a modest start in the 1960s by Dr. Vikram A. Sarabhai – known as the father of Indian space program – the latter has matured in the last six decades through the use of space technologies and applications for national development. Undoubtedly there has been a major evolution since its inception. In this direction, programs and missions developed by the Indian Space Research Organisation (ISRO) consist of launch vehicle development, Earth observation, satellite communications, satellite navigation and space science and planetary

H. Baluragi (✉) · B. N. Suresh

Indian Space Research Organization (ISRO), Bangalore, India, Bangalore, India

e-mail: [baluragi@isro.gov.in](mailto:baluragi@isro.gov.in); [byranasuresh@gmail.com](mailto:byranasuresh@gmail.com); [bnsuresh@isro.gov.in](mailto:bnsuresh@isro.gov.in)

exploration, and satellite applications. One of the important missions accomplished in the recent past is the development and operationalization of the new launch vehicle, GSLV MkIII. India's next milestone mission of Human Spaceflight has been initiated, and the first crewed flight is expected by 2022. As of September 2019, ISRO has accomplished 184 missions, including 101 satellite missions, 73 launch vehicle missions, and 10 technology demonstration missions. This technical chapter describes the evolution of the Indian space program, its dimensions, and new initiatives.

---

## Introduction

The primary objective of the Indian space program is to build indigenous capabilities in space technology, develop applications to meet the developmental needs of the country, and harness the benefits of space applications for socioeconomic development (Suresh 2015; Pant 1986). In this direction, programs and missions drawn up by the Indian Space Research Organisation (ISRO) consist of launch vehicle development, Earth observation, satellite communications, satellite navigation, and space science and planetary exploration. As of September 2019, a total of 184 missions have been accomplished. This includes 101 satellite missions, 73 launch vehicle missions, and 10 technology demonstration missions including Space Capsule Recovery Experiment (SRE), Crew Module Atmospheric Re-entry Experiment (CARE), Reusable Launch Vehicle-Technology Demonstrator, scramjet engine, pad abort test, Indian nano-satellite missions, and microsatellite missions. In addition, 297 foreign satellites from 33 countries have been successfully launched from Sriharikota location using ISRO's Polar Satellite Launch Vehicle.

The Earth observation program consists of state-of-the-art remote sensing satellites such as Resourcesat, Cartosat, Oceansat, radar imaging satellite and weather/meteorological satellites. These satellites observe and monitor Earth's resources and provide systematic information at wide-ranging spatial resolutions available at regular intervals. The satellite communications program includes state-of-the-art INSAT (Indian National Satellite) and the GSAT (Geosynchronous SATellites) communications satellites. These satellites render telecommunication, television broadcasting, meteorological data dissemination, and emergency and strategic communication. They also provide a variety of societal applications for tele-education, tele-medicine, and the Village Resource Centers. The satellite navigation program comprises of a constellation of 8 Indian Regional Navigation Satellite System (IRNSS) with associated ground segment infrastructure. They are intended to provide accurate positioning and timing service supported by the GPS-aided GEO augmented navigation (GAGAN). The space science and planetary exploration program includes satellites designed for studying outer space and planetary exploration; these are the Chandrayaan-1, Mars Orbiter Mission, AstroSat, and Chandrayaan-2.

India has started its launch vehicle development to orbit satellites in a self-reliant manner. Starting with the development of the Satellite Launch Vehicle (SLV-3) during the 1970s, it has progressed through the Augmented Satellite Launch Vehicle

(ASLV), Polar Satellite Launch Vehicle (PSLV), and Geosynchronous Satellite Launch Vehicle (GSLV). Recently, the development of the next-generation launch vehicle, the Geosynchronous Satellite Launch Vehicle Mark III (GSLV MkIII), has been completed and has become operational.

Several other advanced technologies such as the semi-cryogenic boosters and air-breathing propulsion and the development of reusable launch vehicles have been undertaken to meet the long-term demands of the country. Recently, ISRO has initiated the development of a Small Satellite Launch Vehicle toward achieving quick turnaround, on-demand launch services in a cost-effective manner. This vehicle is expected to undergo flight test in the second quarter of 2020. After successful development and demonstration of critical technologies for human space-flight, India has committed to develop end-to-end systems for launch and safe recovery of Indian astronauts by 2022.

---

## Evolution of the Indian Space Program

With a modest start in the early 1960s, the Indian space program has now matured and reached operational stage. From its very inception, the emphasis of the Indian space program has been on the application and utilization of space technology for national development (Suresh 2015; Pant 1986) with gradual transformation in pursuit of self-reliance. Harnessing space applications (Pant 1986) for national development involves:

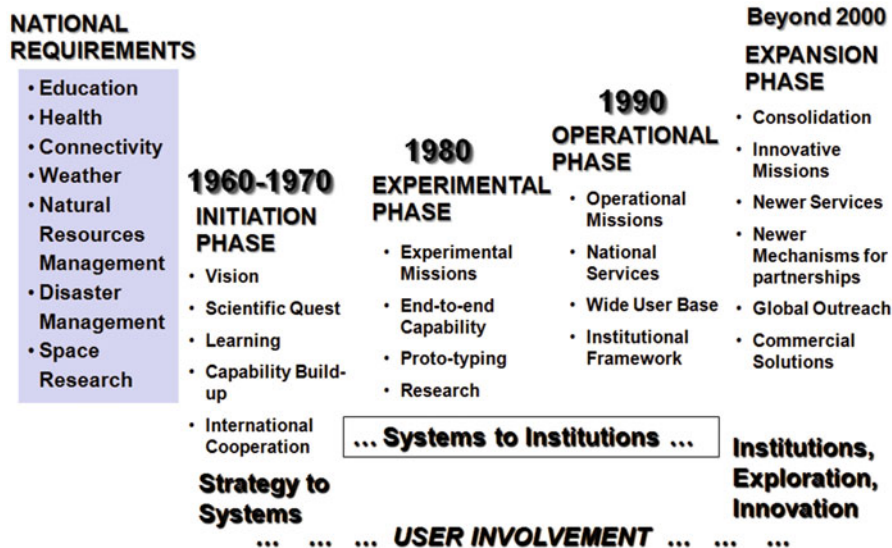
- (i) The use of space for mass communication including communication broadcasted through television and radio, etc.
- (ii) The use of space for navigation
- (iii) The use of space for remote sensing including meteorology to sense, collect, process, and disseminate the resource and weather data for effective use in planning, monitoring, development, and exploitation of natural resources
- (iv) The use of satellites for space science

To realize these goals, the Indian space program has developed capability to (i) carry out efficient utilization of communication and remote sensing satellite data and services; (ii) design, build, and operate communication and remote sensing satellites; and (iii) develop space transportation systems for orbiting satellites. ISRO has made significant progress over the past six decades and has gone through four distinct phases which are shown in Fig. 1.

### Initiation Phase (1960–1970s)

The first “initiation phase” was a learning phase. During this period, ISRO established laboratories, trained manpower by undertaking R&D tasks and took up initial development of sounding rockets and associated scientific payloads. Major





**Fig. 1** Evolution of the Indian Space Program

experimental projects were undertaken for the development of space technology oriented toward applications and appropriate hardware realization. Experiments such as the Satellite Instructional Television Experiment (SITE) and the Satellite Telecommunication Experimental Project (STEP) in the field of space-based communications and broadcasting demonstrated the importance of satellites for national development. The SITE project (during 1975) connected 2400 villages and demonstrated the largest mass communication experiments ever carried out in the world. The STEP project (1977–1979) helped ISRO to understand the problems associated with space and ground systems for telecommunications satellites. To summarize, during this phase, ISRO defined its vision for the space program, strategy for its systems, plan for capability building within the country, and the ability to effectively cooperate with other nations.

**Experimental Phase (1980s)**

In the second “experimental phase,” ISRO developed a series of satellites for different applications such as Aryabhata, Bhaskara-I, Bhaskara-II, and Ariane Passenger Payload Experiment (APPLE). Following the successful demonstration of Bhaskara-I and Bhaskara-II satellites launched in 1979 and 1981, respectively, India began to develop the indigenous Indian Remote Sensing (IRS) satellites to support national development in the areas of agriculture, water resources, forestry and ecology, geology, water sheds, marine fisheries, and coastal management. Toward developing expertise in satellite imagery, ISRO designed and built the first remote sensing missions, i.e., IRS-1A, and launched onboard the Vostok-2M launcher.

Similarly, for technology development of communications satellites, the Indian National Satellite (INSAT) system was commissioned with the launch of the INSAT-1B in August 1983. The INSAT system ushered a revolution in India's television and radio broadcasting, telecommunication, and meteorological sectors. It enabled the rapid expansion of television and modern telecommunication facilities even to remote areas and offshore islands. During this period, ISRO also developed the first-generation launch vehicle SLV-3, which placed the 40 kg Rohini satellite into low Earth orbit, thereby making India the sixth member of an exclusive club of spacefaring nations. The successful culmination of the SLV-3 project showed the way to advanced launch vehicle projects. The Augmented Satellite Launch Vehicle (ASLV) was designed to enhance the payload capacity to 150 kg and enable further technology developments in the areas of strap-on booster, bulbous payload fairing, canted nozzles, closed-loop guidance, and overall mission management. The ASLV proved to be a low-cost intermediate vehicle demonstrating and validating critical technologies needed for future launch vehicles. At the same time, ISRO developed the Polar Satellite Launch Vehicle (PSLV) for the launching of operational remote sensing satellites into the Sun-synchronous polar orbit. For this purpose, it developed state-of-the-art materials and manufacturing methods, and it established a launch pad and major facilities like propellant casting and assembly, integration, and testing.

### **Operational Phase (1990s)**

During the "operational phase," ISRO entered into the operation and quasi-operation of space applications. The INSAT-1 series of the first-generation multipurpose satellites for communication and meteorology and the Indian Remote Sensing (IRS) were launched and made operational. The PSLV provided a quantum jump in the development of critical technologies like large solid motor, Earth-storable liquid engines, composite motor case, strap-down navigation system, etc. This vehicle became a versatile platform for the host of missions such as low Earth orbit (LEO), Sun-Synchronous Polar Orbit (SSPO), and Geosynchronous Transfer Orbit (GTO). In parallel, ISRO initiated the development of Geosynchronous Satellite Launch Vehicle (GSLV) with three stages, employing solid, liquid, and cryogenic propulsion modules for launching 2t class of communications satellites into GTO. Initially, a procured cryogenic stage from Russia was used for the upper stage. At the same time, technology developments needed for the cryo-engine and stage systems were undertaken.

### **Expansion Phase (2000s)**

During the "expansion phase," extending beyond the 2000s, ISRO undertook leapfrog steps in its space program. Apart from capability in design, development, launching, and operationalization of satellite systems, ISRO expanded to undertaking interplanetary missions, reentry missions, commercial launch services,

international collaboration in space technology and advanced technological missions in propulsion, and low-cost access to space. In 2008, India's first space mission to the Moon was achieved with the launch of Chandrayaan-1, which discovered lunar water in the form of ice. The Mars Orbiter Mission (MoM), which entered Mars' orbit on 24 September 2014, made India the first nation to succeed on its maiden attempt to planet Mars. ISRO launched 104 satellites in a single mission (PSLV-C37) – a world record. The cryo-engine developed for the GSLV successfully qualified through a series of ground tests, short and long duration at different levels. The cryo-stage was successfully flight tested in January 2014. The development of the next-generation launch vehicle, the GSLV MkIII, was initiated to meet the demands of launching 4t class of satellites, complete development, and operationalization. Toward future missions of human spaceflight and space science experiments, ISRO successfully conducted the Space capsule Recovery Experiment (SRE). This mission helped to master reentry technologies and recovery procedures required for the design of future reusable launch vehicles. Toward low-cost access to space, the first technology demonstration missions of the Reusable Launch Vehicle (RLV-TD) and scramjet engine were successfully accomplished.

To summarize, India entered into space activities in a humble manner, and over the years it has evolved into a major spacefaring nation through the development and demonstration of all kinds of missions, including interplanetary missions.

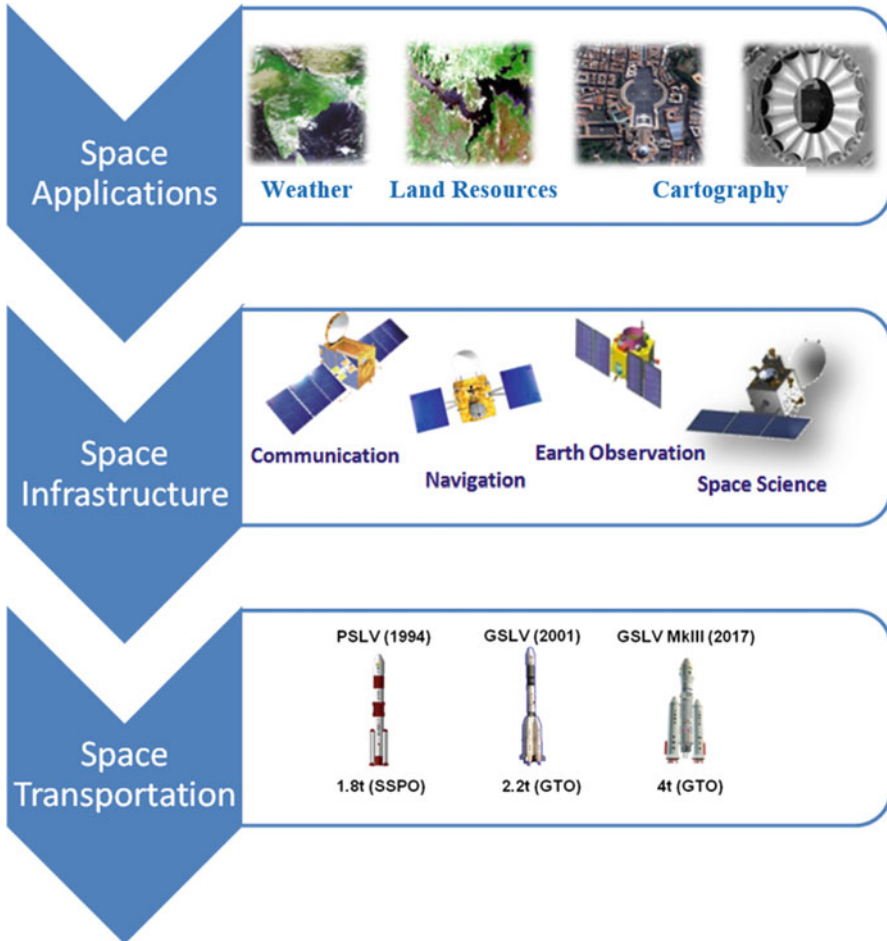
---

## Dimensions of the Indian Space Program

ISRO's programs have always been driven by its vision to "harness space technology for national development while pursuing space science research and planetary exploration." All the space programs till date have aimed at developing independent access to space for which ISRO has developed the PSLV, GSLV, and GSLV MkIII launch vehicles along with the capability to build and operate Earth observation, communication, and navigation satellites. The activities of the Indian space program can be organized into the following dimensions as shown in Fig. 2:

### Space Applications

A major thrust was directed toward space applications right from the very beginning of space activities in the early 1960s. Space applications are derived through synergistic use of Earth observation, communication, and navigation satellites and are complemented with ground-based observations. They play a key role in harnessing the benefits of space technology for socioeconomic security, sustainable development, disaster risk reduction, and efficient governance. Space applications and services in India are tailored to meet the evolving needs and fundamental priorities of the government. Over the past decades, Earth observation data, integrated with in situ observations and tools, have been supporting a host of applications in the areas of land and water, ocean and atmosphere, environment and



**Fig. 2** Dimensions of the Indian Space Program

ecosystem, and urban and rural applications, including disaster risk reduction. Many of these applications have been effectively used and adopted by stakeholder departments for operational use. The capabilities of satellite communications and navigation have also been exploited for delivering an array of societal applications toward education, health, connectivity, skill development, and livelihood sustenance. Besides ensuring continuity of services from space, a strategy has also been drawn to strengthen applications through synergistic use of Earth observation, communication, and navigation satellites. This is planned with a specific focus on harnessing the benefits of space technology in the following broad areas, viz., (i) security of food, water, energy, health, shelter, infrastructure, and information; (ii) sustainable development; (iii) disaster risk reduction; and (iv) governance-related issues. The applications planned in these areas are in tune with the sustainable development

goals, envisaged by the government. Space-based applications and tools are being used by 56 central ministries and governmental departments in planning, periodic monitoring, midcourse correction, and evaluation of developmental activities in various sectors such as agriculture, water resources, forest and environment, urban and rural planning, infrastructure development, satellite communications, and disaster management support. Many flagship programs like the Atal Mission for Rejuvenation and Urban Transformation (AMRUT), the Housing-for-all program, the National Mission for Clean Ganga, the Mahatma Gandhi National Rural Employment Guarantee (MGNREGA), etc. are also utilizing space-based tools. To facilitate these activities, customized tools to stakeholder requirements and mobile applications (Apps) are deployed and used in the current scenario. ISRO is giving further impetus to the utilization of space technology in governance and development by catalyzing the development of innovative applications and services.

## Space Infrastructure

India has painstakingly developed a comprehensive space technology system over the past few decades that has played a significant role in various sectors of national development. Particularly, over the past 30 years, space systems and technologies have increasingly become a critical part in meeting the country's requirements. Space infrastructure includes spacecraft for Earth observation, communication, navigation, and space science, including associated ground segment to ensure data and services on a continued and assured basis. The emphasis has always been on self-reliance in high-technology areas with greater participation of the Indian industries and academia.

The array of Earth observation (EO) satellites that has evolved over a period of three decades with imaging capabilities in visible, infrared, thermal, and microwave regions of the electromagnetic spectrum, including hyperspectral sensors, has helped the country in realizing major operational applications. The imaging sensors have been providing spatial resolution ranging from 1 km to better than 1 m, repeat observation (temporal imaging) from 22 days to 1 day, and radiometric ranging from 7 bit to 12 bit, which has significantly helped in several usages at national level. India has a constellation of 21 EO satellites in orbit. In the coming years, the Indian EO satellites are heading toward further enhanced and improved technologies, taking cognizance of the learnings/achievements made earlier, while addressing newer observational requirements and the technological advancements including high-agility spacecraft.

Communications satellites constitute another vital segment of space infrastructure. Timely realization of multiple communications satellites to meet the national requirements in all sectors will continue to be the core objective of satellite communications program. The INSAT system is one of the largest domestic communications satellite systems in Asia Pacific region with more than 18 operational communications satellites. The INSAT system with more than 250 transponders in the C, Extended C, and Ku-bands provides services to telecommunications,

television broadcasting, satellite news gathering, societal applications, weather forecasting, disaster warning, and search and rescue operations.

Satellite navigation service is an emerging satellite-based system. ISRO is committed to provide the satellite-based navigation services to meet the emerging demands of the civil aviation requirements and to meet the user requirements of the positioning, navigation, and timing based on the independent satellite navigation system. To meet the civil aviation requirements, ISRO is working jointly with the Airport Authority of India (AAI). It established the GPS-aided Geo augmented navigation (GAGAN) system with accuracy and integrity required for civil aviation applications in order to provide better air traffic management of the Indian airspace. To meet user requirements of the positioning, navigation, and timing services based on the indigenous system, ISRO has established a regional satellite navigation system called “NavIC” (Navigation with Indian Constellation) having eight satellites in orbit. Brief details on the NavIC constellation are given in Fig. 3. Expanding the navigation constellation with additional satellites and transforming NavIC system to a global system with improved indigenous time reference system will be one of the main focus areas in the coming years.

The Indian space science program encompasses research in areas like astronomy, astrophysics, planetary and Earth sciences, atmospheric sciences, and theoretical physics. Several scientific instruments have been flown on satellites especially to direct celestial X-ray and gamma-ray bursts. Major science missions undertaken by ISRO include the AstroSat, Mars Orbiter Mission, and Chandrayaan-1 and Chandrayaan-2. The AstroSat satellite is the first dedicated Indian astronomy mission aimed at studying celestial sources in X-ray and optical and UV spectral bands simultaneously. The payloads cover the energy bands of ultraviolet (near and far), limited optical and X-ray regime (0.3–100 keV). One of the unique features of AstroSat mission is that it enables the simultaneous multiwavelength observations of various astronomical objects with a single satellite. The Mars Orbiter Mission (MoM) is ISRO’s first interplanetary mission to planet Mars with an orbiter designed to orbit Mars in an elliptical orbit of 372 km by 80,000 km. The MoM can be termed as a challenging technological mission considering the critical mission operation and stringent requirements on propulsion, communications, and other bus systems of the



**Fig. 3** Constellation and features of NavIC

spacecraft. Chandrayaan-1, India's first mission to the Moon, was orbiting around the Moon at a height of 100 km from the lunar surface for chemical, mineralogical, and photogeologic mapping of the Moon. The spacecraft carried 11 scientific instruments built in India, the United States, the United Kingdom, Germany, Sweden, and Bulgaria. Newer missions to study the Moon, Mars, and Venus are planned in the coming years, including the study of the corona of the Sun (Aditya-L1 Mission).

To provide a platform for standalone payloads for Earth imaging and science missions within a quick turnaround time, ISRO has conceived the small satellite program. Two kinds of satellite buses have been developed, making it a more versatile platform and capable of supporting different kinds of payloads. The Indian Mini Satellite (IMS-1) bus has been developed for 100 kg class satellites which can accommodate a payload capacity of around 30 kg. The first mission of the IMS-1 series was launched successfully on 28 April 2008. YouthSat is the second mission in this series and was launched successfully on 20 April 2011. The microsatellite (Microsat) is a small satellite recently launched by ISRO which is 100 kg and derives its heritage from the IMS-1 bus. This is a technology demonstrator and a forerunner for future satellite technologies. The satellite bus is modular in design and can be fabricated and tested independent of payload. The IMS-2 bus has evolved as a standard bus for 400 kg class that can support payload capacity of around 200 kg. The IMS-2 bus development is an important milestone as it is envisaged to be a workhorse for different types of remote sensing applications in the future. The first satellite based on the IMS-2 bus was SARAL (Satellite with ARGOS and ALTIKA), a joint Indo-French mission launched onboard PSLV-C20 on 25 February 2013.

In order to maximize the impact of the capabilities acquired by the Indian space program and to foster innovation in the space sector, ISRO is following a policy of ensuring the cross-fertilization of knowledge, innovation, and ideas between space and non-space sectors and between space industry and leading research organizations and universities in the country. As part of this policy toward creating a "space-ready" generation, the available spare capacity onboard the PSLV is offered to small satellites built by students of Indian universities, which will enable exposure of the future generation to the multidisciplinary space technology. The first satellite launched in this category was ANUSAT (40 kg) from Anna University, Chennai, on 20 April 2009. As of now, ISRO has provided launch services for ten student satellites from Indian Universities.

## **Space Transportation System**

Assured access to space is a critical goal to a nation's technological advancement, scientific discovery, security, and economic growth. Self-reliance in space transportation systems has been an important component of the guiding vision of the Indian space program in the development of space technology and its applications for societal development. The vision for space transportation systems is to carry forward the self-reliance in launch vehicle technology through increased payload capacity

and reusability. ISRO also envisages to ensure low-cost access to space and progressively arrive at reliable and robust space transportation systems to enable human space activities and space exploration. India has achieved self-reliance in space transportation capability through the operationalization of Polar Satellite Launch Vehicle (PSLV) and Geosynchronous Satellite Launch Vehicle (GSLV) and Geosynchronous Satellite Launch Vehicle Mark III (GSLV MkIII) for launching satellites for Earth observation, communication, navigation, and space exploration.

Evolution of the Indian launch vehicles along with capabilities and achievements are given in Fig. 4. The PSLV has been designed and developed for catering to the need of launching remote sensing/Earth observation satellites into Sun-synchronous and low Earth orbits. The PSLV is configured as a four-stage vehicle with alternate solid and liquid propulsion stages. The first development flight of PSLV was conducted during 1993. The first successful mission of PSLV was in 1994 and orbited a 904-kg Indian Remote Sensing satellite into a Sun-synchronous orbit. PSLV created history by deploying 104 satellites in a single mission. This remarkable achievement was a new moment of pride for the scientific space community and the country. PSLV has so far completed 48 flights which include 3 developmental and 45 operational flights. The 46 flights have been successful, and PSLV has established itself as a reliable and credible launch vehicle. PSLV has successfully orbited 354 satellites of total mass over 50 t. PSLV has demonstrated end-to-end

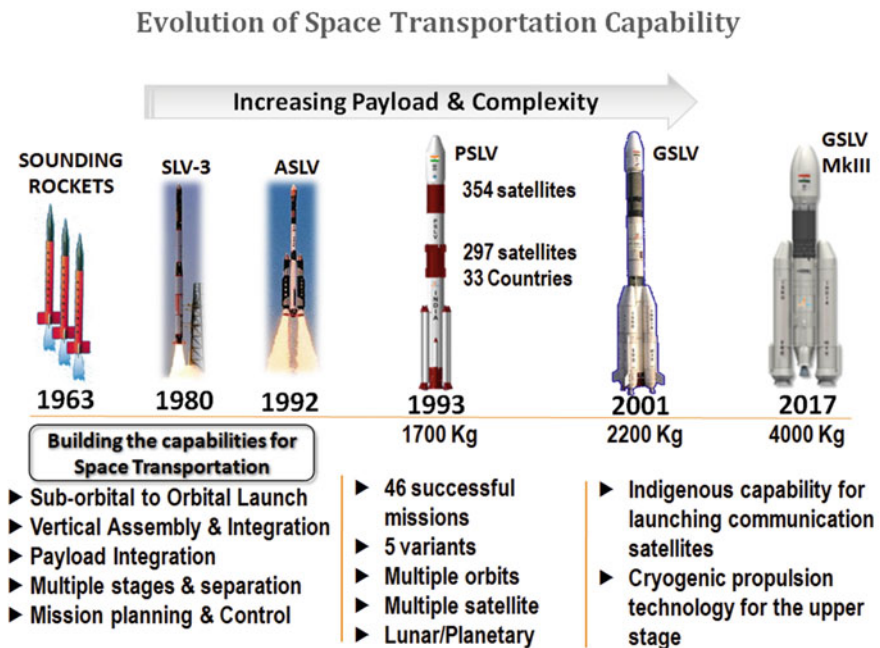


Fig. 4 Evolution of the Indian launch vehicle program



launch services by launching 297 satellites for 33 international customers including 7 dedicated commercial launches. PSLV has become the preferred launcher in the commercial launch market for the payload category up to 1500 kg. In summary, the PSLV has established itself as a workhorse vehicle for national satellites with a capacity that would enable responding quickly to commercial launch opportunities. The target for the PSLV program is to increase the frequency of launches, commercialization of activities through industry, and improvement of the global competitiveness through cost reduction measures.

The Geosynchronous Satellite Launch Vehicle is an expendable launch vehicle, designed and developed to launch 2t class of satellite to 180 km by 36,000 km geostationary transfer orbit. GSLV is a third-generation launch vehicle. It is a three-stage vehicle with four liquid strap-ons and cryogenic upper stage (CUS). GSLV uses main systems that are already proven in the PSLV in the form of solid booster and liquid-fueled Vikas engine. The first developmental flight of GSLV, i.e., GSLV-D1 carrying a payload of 1540 kg, was launched successfully on 18 April 2001. GSLV's primary payloads are 2t class of communications satellites that operate from geostationary orbits. The GSLV with indigenous cryogenic stage (GSLV-D5) was successfully launched on 5 January 2014 and has placed the GSAT-14 spacecraft with a mass 1980 kg in GTO. This was a major milestone for the Indian Space Research Organisation and a very significant demonstration of complex cryogenic technology. One of the significant achievements of the GSLV program, as a whole, is the development of complex cryogenic technologies, comprising of system design for engine and stage, special manufacturing process, new material development, testing facilities for subsystems, engine and stage and launch pad propellant filling, etc. The experience thus gained in CUS paved the way for the indigenous design and development of bigger engine and stage for the GSLV MkIII program and is also the stepping stone for the next-generation semi cryo-engine and stage development.

The Geosynchronous Launch Vehicle Mark III (GSLV MkIII) is a fourth-generation launch vehicle developed by ISRO primarily developed toward achieving indigenous launch capability to launch 4t class of communications satellites into geosynchronous transfer orbit (GTO). It is also identified as launch vehicle for crewed missions under Indian Human Spaceflight Programme. GSLV MK-III is configured with two solid strap-on motors (S200), one liquid core stage (L110), and a high thrust cryogenic upper stage (C25). The S200 solid motor is among the largest solid boosters in the world with 204.3 t of solid propellant. The liquid L110 stage uses a twin liquid engine configuration with 115.4 t of liquid propellant, while the C25 cryogenic upper stage is configured with the fully indigenous high thrust cryogenic engine (CE20) with a propellant loading of 28.35 t. The overall length of the vehicle is 43.5 m with a gross lift-off weight of 640 t and a 5-m diameter payload fairing. The first developmental mission of GSLV MkIII (GSLV MkIII-D1) was completed successfully on 5 June 2017, which launched the communications satellite (GSAT-19) into GTO orbit. So far, the GSLV MkIII vehicle has completed three missions, and all were successful.

## The Human Spaceflight Program: A New Beginning in the Indian Space Program

In the early years of human spaceflight, progress was fast owing to the race for technological supremacy between the United States and the then Soviet Union. The competitive spirit drove the space engineers from these two nations to develop technologies for human spaceflight of increasing complexity including the launch vehicles, space capsules, reentry, and recovery strategies, which are all relevant to this day. While the early phase of the program till the early 1980s was focused on competitive technology development and demonstration, the next phase of the human spaceflight started incorporating science objectives with several science experiments conducted on the early Space Stations. This was followed by an era of international cooperation between the major space powers, which gave rise to the International Space Station (ISS), which has been the focus of human activity in space since 1998. ISS has been serving as a platform for evaluating human endurance in space, microgravity research, and interdisciplinary research till date. Human spaceflight capability in terms of launch capability, crew and habitat module, and safe return from orbit has been developed by the United States, the USSR, and China. From 1961 to 2018, more than 300 human spaceflight missions have been conducted by the United States, the USSR, Russia (Post 1991), and China. In recent times, there is a renewed interest in human space exploration through a globally coordinated approach synergizing the capabilities of all spacefaring nations and private players targeting exploration of the Moon, Mars, and near-Earth objects (asteroids) along with extraterrestrial resource exploitation.

Toward achieving indigenous capability in human transportation, ISRO conducted a major technology demonstration (Kumar et al. 2018) on 5 July 2018, the first in a series of tests to qualify a crew escape system, which is a critical technology relevant for human spaceflight. Launch phase of crew escape system and recovery using parachutes are shown in Fig. 5. The crew escape system is an



**Fig. 5** Pad abort test of crew escape system

emergency escape measure designed to quickly pull the crew module along with the astronauts to a safe distance from the launch vehicle in the event of a launch abort. The crew escape system, weighing 12.6 t with the simulated crew module was lifted off using the specially developed solid motor with multiple reverse flow nozzle. In this test, the crew escape system along with the crew module was accelerated at 10 g and reached to a maximum altitude of 3 km. Recently, on 15 August 2018, the Prime Minister of India formally announced the Gaganyaan project, an Indian Human Spaceflight Programme which has given major push in this area. The Gaganyaan project is a fully autonomous 3.7-t spacecraft designed to carry a 3-member crew to orbit and safely return to the Earth after mission duration of up to 7 days. The crew module is mated to the service module, and together they are called the orbital module. The composite module of crew module and service module will have the Environmental Control and Life Support Systems (ECLSS) to ensure that conditions inside the crew module are suitable for humans to live comfortably. The ECLSS maintains a steady cabin pressure and air composition, removes carbon dioxide and other harmful gases, controls temperature and humidity, and manages parameters like fire detection and suppression, food and water management, and emergency support. Recovery and reentry aspects have been demonstrated in the Crew Module Atmospheric Reentry Experiment (CARE) that was flown onboard experimental flight of GSLV MkIII (LVM3-X) during December 2014. In this technology demonstration mission, a CARE module reentered the atmosphere at about 80 km altitude and landed in the sea, from where it was recovered by the coast guard. Many such experimental flights are planned before manned flight.

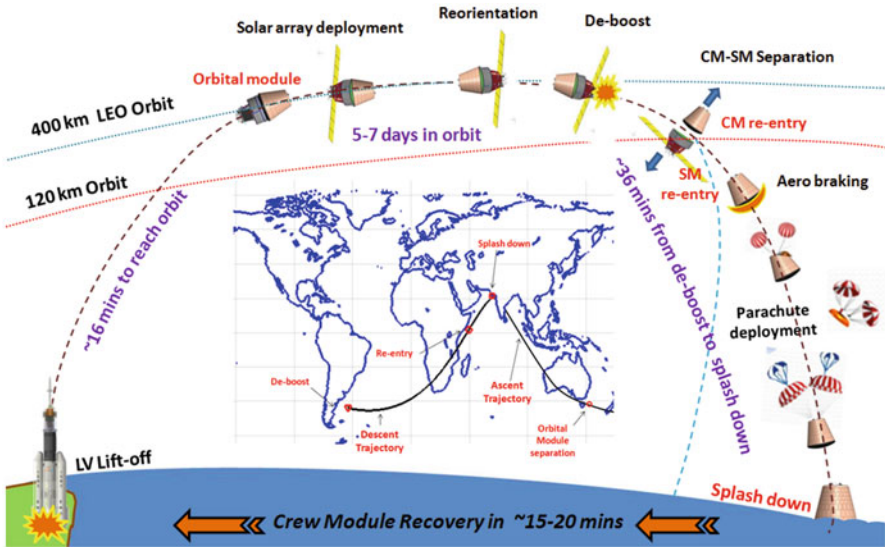


Fig. 6 Mission profile of Gaganyaan project

Based on the payload capacity, ISRO has chosen the GSLV MkIII launcher for orbiting the crew and service module. The GSLV MkIII will be human rated by incorporating improvements in the stage systems. The Launch Vehicle is also equipped with emergency mission abort and emergency escape that can be done during the action of first stage or second stage of the launch vehicle. The mission profile for Gaganyaan project is shown in Fig. 6.

Following two non-crewed orbital flight demonstrations, a crewed Gaganyaan is scheduled to be launched on the GSLV MkIII launcher by 2022.

---

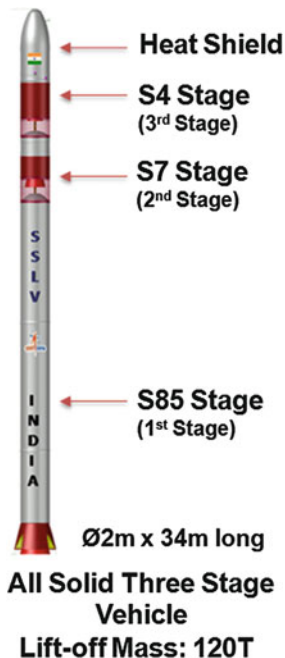
## **New Initiatives Toward Low-Cost Access to Space**

Currently, bringing down the cost of access to space is a primary goal of space programs around the world. After successful operationalization of the Polar Satellite Launch Vehicle (PSLV), the Geosynchronous Launch Vehicle (GSLV), and the Geosynchronous Launch Vehicle Mark III (GSLV MkIII), ISRO is in the process of developing a Reusable Launch Vehicle technologies to achieve low-cost access to space. Toward this program, a winged body configuration was conceived, which can fly at subsonic, supersonic, and hypersonic Mach number regime, reenter into Earth atmosphere, and land. ISRO is also developing technologies for air-breathing engine that uses atmospheric oxygen along with kerosene fuel to generate required thrust. A Small Satellite Launch Vehicle is being developed to provide on-demand launch at low cost.

### **Small Satellite Launch Vehicle**

Traditionally, small satellites (below 500 kg) are launched as co-passengers along with primary satellites. In this situation the primary satellite takes the priority, and the small satellites have to be adapted to the launch schedule and orbit. This results in increased waiting time, non-optimum orbits (of primary spacecraft) that are far from ideal for the smaller spacecraft and do not always meet the unique requirements of planned missions. The small satellite industry has witnessed a rapid growth in the last few years. According to Euroconsult's recent report (Euroconsult 2019), nearly 8500 satellites will be launched worldwide over the next 10 years for government and commercial requirements. The estimated market value for small satellites manufacturing and launch is \$13 billion with a potential growth rate of 13% per year. The launch of small satellites during the past decade is constrained by a limited number of launch vehicles. Innovation in miniaturization and standardization of satellite parts has trimmed the satellites' size and costs substantially. This has made feasible the building, launching, and operation of small satellite constellations. Nearly 33 small satellite launchers are under development worldwide, which are capable of offering 150–750 kg to LEO.

For catering the above requirements, ISRO has taken up the development of a cost-effective launcher, the Small Satellite Launch Vehicle (SSLV) that can offer

**Fig. 7** SSLV configuration

mission flexibility and on-demand launch. The SSLV is a three-stage solid propellant-based vehicle (S85 + S7 + S4) with a liquid velocity trimming module having payload capacity of 400–500 kg to LEO (500 km planar). The configuration of SSLV is given in Fig. 7. New technology developments for small satellite launch vehicles include the flexible nozzle driven by electromechanical actuator for solid motors, miniaturized avionics, stage separation system based on expandable tube assembly, etc. The design for all solid motors of SSLV is based on already well-proven solid motors of PSLV and GSLV launch vehicles. Propellant casting for all solid motor stages, subassembly preparation and testing, stage integration and testing, and vehicle integration and launch are planned with minimal infrastructure and manpower. The first development flight of the SSLV is expected during the second quarter of 2020.

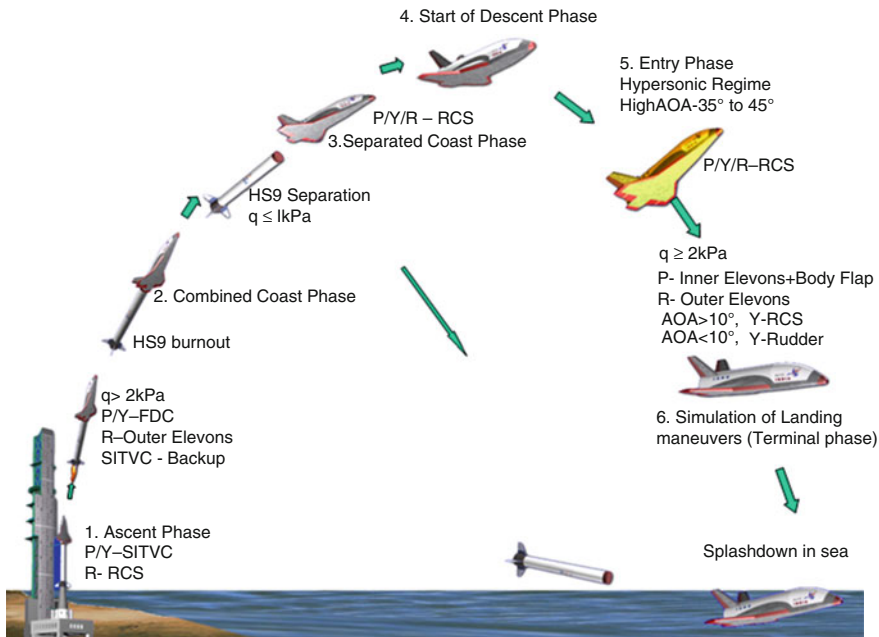
## Reusable Launch Vehicle: Technology Demonstrations

Reusability of space transportation systems, or at least parts of it, is the key capability to achieve for a significant cost reduction and quick turnaround operations. Reentry technology demonstrator missions (Sivan et al. 2018) have been discussed widely in the literature. The ALFLEX, HYFLEX, and OREX of JAXA, the X-43A and X-51A of NASA, and the IXV of ESA are some examples. Many countries had embarked into RLV programs since the 1980s. A viable technology that is fully reusable and brings down launch costs is yet to emerge in the global

launch market. Yet, this may be changing with the advent of the recent innovative recovery approach and reusability of the booster by the Space Exploration Technologies Corporation (SpaceX).

ISRO conceived a scale-down wing body technology demonstrator to acquire and validate the hypersonic vehicle design process as a first step toward full-scale space plane. The hypersonic experiment technology demonstrator vehicle (RLV-TD) was successfully flight tested (Sivan et al. 2018) in May 2016. The RLV-TD configuration in this mission is unique, because the double-delta wing body demonstrator was placed on top of the 11-m long and tailor-made slow-burn-rate solid booster. The mission profile for RLV-TD is given in Fig. 8.

Similar winged body flights were done by the National Aeronautics and Space Administration (NASA) and the European Space Agency (ESA). The major difference as compared to RLV-TD mission is that NASA and ESA have conducted it accommodating the winged body inside (Sivan et al. 2018) a heat shield. The RLV-TD mission was also unique because it was designed to minimize the cost and to get the maximum data in a single mission itself. In order to prepare the technology needed for the timely development of the fully reusable launch vehicle that may be required in the longer term and may be crucial for future space activity, ISRO has planned an in-flight experiment of a winged body orbital vehicle mission during the next 2–3 years. Prior to orbital mission, a series of landing experiments of the vehicle are planned to be carried out on the runway through autonomous control with a high degree of lateral accuracy, which calls for highly precise navigation system



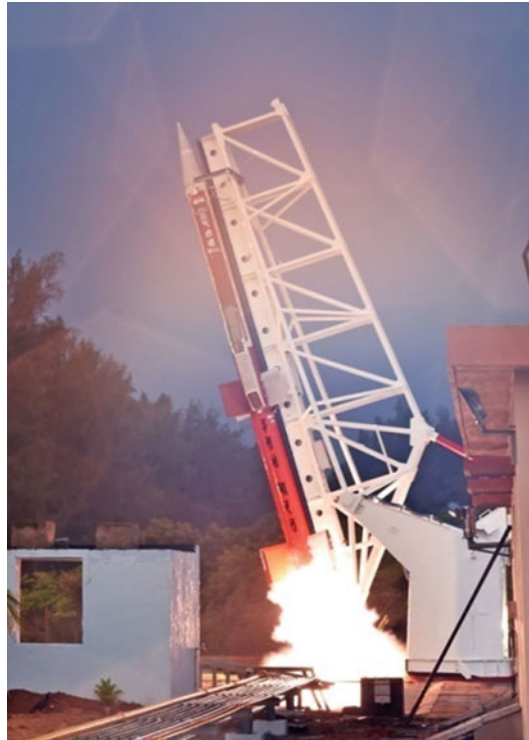
**Fig. 8** Mission profile of RLV-TD

consisting of an onboard GNSS-aided Inertial Navigation System, pseudolite systems, and precise radar altimeters.

## Hypersonic Air-Breathing Engine

The scramjet engine technology on air-breathing propulsion has the potential to increase the payload fraction, low-cost access to space, and launch frequency. So far very few nations (Mishra et al. 2018), namely, Russia, the United States, Australia, and India, have conducted scramjet demonstration programs. Various scramjet engine testing demonstration programs undertaken are the Kholod program (Russia), X-43A and X-51A (USA), Hyshot and HiFire (Australia), and SCRAMJET (India). The various air-breathing vehicle development programs proposed worldwide are the SPARTAN (Australia), GTX (USA), Skylon (UK), and AB-RLV (Japan). Selecting a suitable platform for flight testing of scramjet engine is important as the scramjet experiment has to be carried out in a particular flight environment governed by Mach number and dynamic pressure combination. The X43-A Hyper-X scramjet technology demonstrator was mounted on a booster (modified 1st stage of Pegasus rocket) that was air launched from the mother ship Boeing B52 aircraft. The booster was guided and controlled to achieve desired combination of Mach number

**Fig. 9** Scramjet engine: technology demonstrator



and dynamic pressure for scramjet experiment. The Australian scramjet experiment Hyshot was done on a ballistic trajectory of sounding rocket.

ISRO has conducted two technology demonstration tests (Mishra et al. 2018), i.e., ATV-D01 and ATV-D02 in March 2010 and August 2016, respectively, in which a basic understanding of engine configuration and its ignition under higher Mach number have been flight demonstrated successfully. The technology demonstrator for scramjet engine is shown in Fig. 9. With regard to the overall development of a scramjet engine capable of generating positive acceleration, ISRO is working on critical technology development for hypersonic air-breathing vehicle with airframe-integrated test vehicle and demonstrated scramjet technology for long duration.

---

## Conclusion

It was the vision of Dr. Vikram A. Sarabhai who initiated the Space Program in India in the 1960s, to utilize the potential of space technology and its applications for national development. The Indian space endeavor had a modest beginning with the launch of the sounding rocket from Thumba on 21 November 1963. Since then, in the last five decades, India has made considerable progress in the development and operationalization of satellites and space launch vehicles. With satellite constellation in LEO and GTO orbits along with ground systems, ISRO exploits the full potential of space technology for national development. The primary thrust of ISRO will be to maintain and improve national development and, at the same time, to achieve the desired self-reliance in meeting the future requirements of space infrastructure, space transportation systems, and ground systems.

---

## References

- Euroconsult (2019) Prospects of Small Satellite market – forecasts to 2028. <http://www.euroconsult-ec.com/research/SS19-brochure.pdf>. Accessed 10 Dec 2019
- Government of India (2019) Department of Space, Indian Space Research Organization (ISRO). <https://www.isro.gov.in/>. Accessed 10 Dec 2019
- Kumar K et al (2018) Overall mission performances of crew escape system – Pad abort test flight, ASCEND. In: National system conference 2018 by Systems Society of India, Trivandrum Chapter
- Mishra P et al (2018) Mission design challenges in sounding rocket based scramjet engine test vehicle. *J Aerosp Sci Technol* 70(3A):195–202
- Pant N (1986) Indian space program. *Indian J Radio Space Phys* 15:402–432
- Sivan K et al (2018) An overview of reusable launch vehicle technology demonstrator. *Curr Sci* 114 (1):38–47
- Suresh BN (2015) The Indian space launch program. In: Schrogl K-U et al (eds) *Handbook of space security: policies, applications and programs*. Springer, New York





Michael Davis and Chris Schacht

## Contents

Introduction .....	1442
Australia's Dependence on Space .....	1443
National Security and Space .....	1444
Australian Defence Policy .....	1445
Defence Integrated Investment Program .....	1447
Next Generation Technologies Fund .....	1448
Launches from Australia .....	1449
Equatorial Launch Australia .....	1449
Southern Launch .....	1450
Gilmour Space Launch Services .....	1450
Conclusion .....	1452
References .....	1452

## Abstract

The space sector in Australia is experiencing an unprecedented level of public interest and government support. National security considerations as well as the economic benefits of a fast-growing world market for space products and services are inextricably linked as drivers for a range of government and industry initiatives outlined in this chapter. After decades of wavering government support for the space sector in Australia, there are signs that a coherent public program of capability development and R&D support, commensurate with Australia's

---

M. Davis (✉)  
Space Industry Association of Australia, Adelaide, Australia  
e-mail: [mdavis@spacelaw.com.au](mailto:mdavis@spacelaw.com.au)

C. Schacht  
Adelaide, Australia  
e-mail: [Australiaschacht@ozemail.com.au](mailto:Australiaschacht@ozemail.com.au)

strategic and social needs, is emerging. The programs and initiatives outlined in this chapter are driven in part by a greater understanding of the national security dependencies and risks that Australia as a nation is exposed to and provide evidence that Australia is now treating space as an integral component of its role in the protection of its national security interests and in the advancement of its international responsibilities.

---

## Introduction

The space sector in Australia is experiencing an unprecedented level of public interest and government support. National security considerations and the economic benefits of a fast-growing world market for space products and services are inextricably linked as drivers for a range of government and industry initiatives outlined in this chapter.

On the civil side, in July 2017 the Australian Government announced a review of Australia's space industry capability to ensure that Australia was able to "capitalise on the increasing opportunities within the global space industry sector." In its Interim Report in August 2017, the Expert Review Group appointed by the Government stated that:

Australia has billions of dollars' worth of space-related existing infrastructure and facilities, a vibrant community of over 50 small companies and over 40 medium-sized companies active in the space sector . . . world-leading capability including in research, satellite data analysis, radar and radio communications, and several emerging areas of strength. ([Review of Australia's Space Industry Capability](#))

The Expert Review Group further concluded that "there is a need for a single point of contact for domestic and international partnerships, greater national coordination and strategic direction, government support to enable industry to participate in global supply chains, and a whole-of-government approach to the space sector (Ibid., pp. 68 and 69)." The stakeholder consultations carried out as part of the review revealed that there was a strong call for a space agency with the authority to coordinate Australia's space activity and to focus on the following requirements:

1. A national strategy that builds on national strengths and identifies areas of focus for Australia in the space sector
2. The coordination of domestic activities in Australia's space sector ensuring that Australia has the space capabilities to meet its strategic needs and manage risks associated with its space-related dependencies
3. A single point of contact for international engagement and partnerships with a clear point of contact within the Australian Government that can actively engage with global partners to maintain critical partnerships and broker future space opportunities
4. Support for the development of Australia's space industry capability

The Interim Report added that the space agency should be “modest, forward-looking and agile.” It was not proposed that the space agency should take over the operational and regulatory activities currently being undertaken by other existing authorities. It was further said that “the future direction in space is in partnership with the private sector, as has been demonstrated through the Canadian and UK space programs.”

The key recommendation for the establishment of a national space agency was quickly accepted by the Australian Government. Following on that, on 25 September 2017 at the Opening Ceremony of the International Astronautical Congress in Adelaide, the Government announced that an Australian Space Agency would be established ([Space News](#)).

This decision was seen as an important step forward for Australia and was a welcome response to the widely held view among key industry players that the development of a mature and innovative Australian space sector and a level of sovereign space capability underpinned by world class space science and technology had become an urgent national priority, taking into account:

1. The fact that the Australian Government was committed to taking advantage of innovation in science and technology to transform the national economy and strengthen security
2. The perception that Australia was missing out on opportunities enjoyed by other advanced economies in an industry sector that was enjoying growth rates exceeding 10% per annum
3. The belief that Australia could no longer assume that its vital security interests in space will continue to be maintained at virtually no cost to the Australian Government ([Space Industry Association of Australia](#))

---

## Australia's Dependence on Space

For over 60 years, space has played an important role in national affairs and international relations in Australia. Space-derived data and services have increasingly become embedded into the fabric of modern life providing the communications, geolocation, and timing services upon which millions of individuals and businesses rely each day. They include satellite positioning and communication services, as well as satellite earth observation and astronomy capabilities. A White Paper published by the Space Industry Association of Australia (*Ibid.*) concluded that without space technologies:

- Australia's ability to forecast weather and extreme weather events is immediately compromised, reducing the capacity to respond to emergencies such as bushfires and floods.
- Communications services, including Foxtel, Imparja, the National Broadband Network, and general telephony, would be significantly affected, leaving

Australia reliant on a very small number of undersea cables for connection to the outside world.

- Smartphones would not provide positioning data, with Google Maps, Uber, and any other GPS-based apps immediately useless.
- Telecommunications, critical in providing health and education support in remote communities, would suffer.
- Farmers would no longer be able to use precision agriculture, and the supply and delivery of food could no longer be coordinated through space-based navigation.
- Mining companies would lose a valuable exploration method.
- Air traffic would be disrupted.
- Financial transactions which rely on GPS satellites would slowly degrade.
- Defence would lose satellite communications, intelligence satellites, and GPS, critically affecting their ability to protect and defend Australia and its borders.

The SIAA White Paper went on to state that “. . .Australia has benefited greatly from access provided by partner nations such as the United States, Japan and Europe for much of its satellite data, and traditionally this has been at very little cost to the Australian Government. There are numerous examples of the economic and societal benefits generated from earth observation (EO) data in Australia, across areas such as weather forecasting, onshore and offshore mining, mitigation and management of natural disasters like bushfires and floods, water resource management, design and assessment of conservation areas, insurance assessment, and land use planning. . .Our public and private sectors are fundamentally dependent on EO which is entirely provided by other countries. These data and services are recognised as essential to our public and private infrastructure with numerous national reviews showing that Australian governments and industry are critically dependent on EO to maintain our economy and societal wellbeing. There is a vital national interest in maintaining the infrastructure, capabilities and international relationships necessary to secure access to satellite data sources.”

The Space Industry Association of Australia document concluded that “A key issue in the development of our national space policy should therefore be the securing of long-term access, for strategic purposes, preferably from Australian territory, to foreign owned space-segment capabilities, both military and civil. Furthermore, as the geo-political environment changes, Australia needs to become a technology contributor to those partnerships, or it risks significantly rising costs or, even, loss of access. Australia would also be well-advised to consider ways to reduce its dependence on the traditional data sources, and consider its own national priorities in the development of new systems.”

---

## National Security and Space

There is an increasing awareness in Australia of the social and political implications of the country’s dependence on space assets and services.

As one commentator put it, "...Australians have grown used to living in a just-in-time world for energy supply, logistics, power, heating and cooling to the point that it's only when the lights go out in Tasmania or South Australia that people realise there's a complex but imminently vulnerable interconnected system of supply and distribution that sets the rhythm of our lives. And so much of this depends on access to and control of space. While our military forces think about the implications of operating in a 'day without space', our politicians should ponder what a day or two without space would do for the quality of social harmony in Australia. If satellites go down and there are no others that can provide redundancy and resilience, how long would it take to turn our urban centres into end-of-days theme parks?" ([Australian Strategic Policy Institute](#)).

In a similar vein, another international commentator has observed:

Firstly, the sheer number of potential satellites planned will tax existing collision deconfliction and traffic management structures. On current forecasts, the number of active satellites will increase in the next decade, from approximately 1,800 to a number approaching 10,000. Within this range, a number of 'mega-constellations' are proposed, each containing thousands of satellites. Much of the explosion in numbers is forecast to occur within a fairly constrained orbital regime, within 1,000 kilometres of the surface of the earth.

Such developments may quickly overtake the current means of space surveillance, which is based around the independent verification of orbits by agencies like the US Space Surveillance Network, and in the future the US Department of Commerce. Increasingly, the best source of orbital information will be the operators themselves, which will require new ways of exchanging and verifying such data. Once exchanged, agreed norms of orbit maintenance and deconfliction measures will need to be established between operators. Additionally, the real-time monitoring and adjustment of constellations within a congested environment will drive a level of system autonomy currently unseen in current operations.

Added to this, the increasing miniaturisation of spacecraft—exemplified by the growth of 'cubesats'—will challenge the ability of existing surveillance systems to track and identify objects in orbit. The distribution of missions across multiple satellites has meant a steady reduction in object size, while modular construction techniques will make more satellites appear alike to external ground- and space-based observers. ([Australian Strategic Policy Institute](#))

---

## Australian Defence Policy

Since the 2016 Australian Government Defence White Paper ([Australian Government, Department of Defence](#)), there has been official recognition in Australia that access to space is important to the strategic interests of the nation. This key defence policy document proposes the continuing expansion of Australian space-based and space-enabled capabilities over the next 20 years, with space surveillance projects to be the "acquisition pipeline to strengthen Defence's awareness of space ([Australian Strategic Policy Institute](#)).” The Government's clear intention is to enhance Australian Defence sovereign space capabilities progressively through access to allied and commercial space-based capabilities (*Ibid.*).

As one commentator put it, “. . . a new factor driving national approaches to space is that all countries are faced with an increasingly stark choice to ‘use or lose’ their interests in space. Australia is acquiring at immense cost a fifth-generation-enabled defence force which, if we’re ever to fight with it, must have assured access to systems that rely on space. The US alliance provides fantastic access to key space systems; however, it could benefit from increased resilience from allied systems designed with it in mind. So a defence policy for space must set out how we’ll ensure that our forces have access to key systems inside our alliance with the United States and alone if necessary (Ibid.)”

The close strategic alliance between Australia and the United States features prominently in Australia’s space-related capability planning. According to the Australian Strategic Policy Institute, “[a] key task is to determine how best Australia can work alongside the United States and other partners to deter threats to our critical space capabilities, and if necessary to mitigate the effects of warfare in space.”

This is in stark contrast to the traditional approach in which Australia had been content to be dependent on foreign providers for space capability. According to the Australian Strategic Policy Institute, “For much of the period from the 1960s onwards, Australia adopted a supporting role in space—providing a suitable piece of real estate for ground facilities, supplying skilled personnel and managing the data coming from the satellites. However, we’ve not done anything significant in terms of developing sovereign capability in terms of ‘the space segment’ ([Australian Strategic Policy Institute](#)).”

For defence and national security, space is a vital domain. Space is no longer a pristine global common that’s a sanctuary from warfare. In the 21st century, it’s recognised to be a warfighting domain that’s ‘contested’ through the growing threat of adversaries’ counter-space capability. It’s also increasingly ‘congested’ as a result of growing space debris. Finally, space is increasingly ‘competitive’ as new approaches to space activities such as Space 2.0 see the acquisition of space capabilities by a broader range of state and non-state actors. Space is no longer dominated by only the major powers, and the impact of the private sector is clearly visible every time SpaceX launches—and then lands—one of its rockets.

Ensuring access to space is vital to Australia’s defence capability and to our approach to military tasks. Without an ability to access space capabilities—either our own, or those of an ally—our ability to fight and win information-based warfare and undertake ‘multi-domain operations’ is severely limited, and our adversaries are better placed to impose costs or even military defeat against our forces. (Ibid.)

The rationale for the development of defence space-related capability as set out in the White Paper and related documents is that the Australian Defence Force is reliant on space-based satellite systems to support its networked capabilities and to communicate and fight when deployed on operations. The documents note that some countries are developing capabilities to target satellites to destroy these systems or degrade their capabilities, threatening these networks. Space-based capabilities also offer potential adversaries advanced information gathering opportunities, including imagery gathering. The availability of commercial space-based systems also means that smaller countries, private interests, and non-state actors can access sensitive information about our security arrangements, such as imagery of Defence bases.

To ensure the security of its space-enabled capabilities, the Australian Government's stated policy is to strengthen Defence's space surveillance and situational awareness capabilities, including through the space surveillance radar operated jointly by Australia and the United States, and the relocation of a US optical space surveillance telescope to Australia.

It is also noted in the White Paper that “. . . [l]imiting the militarisation of space will also require the international community to work together to establish and manage a rules-based system – a prospect that does not seem likely in the immediate future.”

In order to achieve these aims, the Australian Government has decided to strengthen its defence capability in six capability streams. One of these streams, “intelligence, surveillance, reconnaissance, space, electronic warfare, and cyber,” is designed to ensure that Defence Forces have superior situational awareness.

---

## Defence Integrated Investment Program

The Defence White Paper outlines a 10-year Integrated Investment Program under which approximately AUD195 billion was allocated in the decade to 2025–2026 for investment in new and enhanced capabilities. This includes investment in “space-related capability, including space-based and ground-based intelligence, surveillance and reconnaissance systems; and space situational awareness and command, control, communications, computer and intelligence capabilities ([Australian Government](#)).”

The Defence White Paper states that “Space-based systems for intelligence collection, communications, navigation, targeting and surveillance play a vital role in all Australian Defence Force (ADF) and coalition operations. Defence's imagery and targeting capacity will be enhanced through greater access to allied and commercial space-based capabilities, strengthened analytical capability and enhanced support systems. Enhancements to our imagery capacity will provide the basis to further develop our intelligence, surveillance and reconnaissance capabilities in the longer term, including through potential investment in space-based sensors.”

The Defence White Paper further notes that:

- Satellite systems are vulnerable to space debris, which could damage or disable satellites, and advanced counter-space capabilities, such as anti-satellite missiles, which can deny, disrupt, and destroy space-based systems. It is therefore important to be able to detect and track objects in space so Defence can plan to manage the effects of any possible damage to our space-based capabilities.
- In cooperation with the United States, Australia is strengthening its space surveillance and situational awareness capabilities. At the center of this work are the establishment of the space surveillance C-band radar operated jointly by Australia and the United States and the relocation of a US optical space surveillance telescope to Australia. (Both assets will be located at the Harold E. Holt Naval Communications Station near Exmouth in Western Australia.)

- The Government intends to upgrade the Australian Defence Force's existing air defence surveillance system, including command, control and communications systems, sensors, and targeting systems, "which could be used as a foundation for development of deployed, in-theatre missile defence capabilities, should future strategic circumstances require it." The Government will also acquire new ground-based radars from around 2020 and will expand Australia's access to situational awareness information, including space-based systems.
- The Government also intends to upgrade facilities at the Harold E. Holt Communications Facility in Exmouth, Western Australia, to support enhanced space situational awareness and communications capabilities and will similarly upgrade the Jindalee Operational Radar Network and other surveillance and air defence-related facilities in northern Australia.

Other space-related initiatives flowing from the Defence White Paper include improved capability in satellite imagery analysis and space situational awareness. The 2016 Integrated Investment Program document notes the following:

#### *Imagery*

Australia's ability to collect and use imagery data will be substantially enhanced, including increasing the capacity for imagery analysis. This will be achieved primarily through additional personnel and equipment for the Australian Geospatial-Intelligence Organisation, and enhanced access to imagery, including imagery from satellites.

Australia will continue to invest in expanding access to geospatial data through both existing and new commercial and partner arrangements. This data will enhance our support to regional and global operations, and improve the resilience of our access to space-derived information, including operational imagery and targeting.

#### *Space situational awareness*

Australia's existing space situational awareness capability relies on access to comprehensive United States-sourced and processed space situational awareness information. Existing arrangements will be strengthened through the relocation of the C-band radar and optical space surveillance telescope to Australia, enhancing our access to space situational awareness information. Defence will also examine other ground-based sensors, including radar and optical systems, to develop options for expanding Australia's space situational awareness sensor coverage in the future.

---

## **Next Generation Technologies Fund**

According to the 2018 Defence Industrial Capability Plan ([Australian Government](#)), the Department of Defence's nascent space programs will be developed into national capabilities over the next 10–15 years, and opportunities for industry and research institutions exist "in the design, delivery and operation of space situational awareness, satellite imagery, space operations and big data management and analytics capabilities."

The Plan states that "The Government's investment of \$730 million over 10 years through the Next Generation Technologies Fund is an unprecedented opportunity to



deliver high-impact future capabilities for Defence by tapping into the talent and innovation in Australia's industry and academic institutions (Ibid., paragraph 4.37)."

The Fund will support a range of collaborative projects with academia, industry (both small and large), publicly funded research agencies, Defence Science and Technology Group scientists, other areas of Defence, and Australia's allies.

Approaches to partnering between Defence and Australian innovators under the Next Generation Technologies Fund include:

- A Grand Challenge Program – bringing together government, industry, and academia to solve large-scale research problems of strategic importance to national security.
- A Defence Cooperative Research Centre Program – driving research partnerships to address high-priority defence technologies and to develop commercially viable products and solutions for future defence capabilities.
- A Small Business Exploratory Research Program – to accelerate promising science and technology of interest to the Defence, from early-stage concept development to a point where the research and technology could transition to the Defence Innovation Hub.
- A US-Australia Multidisciplinary University Research Initiative (AUSMURI) – a research network which is investing \$25 million over 9 years for grants to support Australian participation in the already established US MURI program. Multidisciplinary teams of Australian university researchers collaborate with US academic colleagues on high-priority projects for future defence capabilities.

---

## Launches from Australia

In its final report delivered in March 2018, the Australian Government's Expert Reference Group recognized that space launch capability is an industry enabler and recommended the new space agency should facilitate "regulatory approval processes for small satellite launch facilities in Australia and the launch of Australian satellites overseas" and investigate opportunities to partner with appropriate international launch providers ([Review of Australia's Space Industry Capability](#)). Interest in Australia for the development of commercial launch services has since increased, and recent project announcements include the following:

### Equatorial Launch Australia

Equatorial Launch Australia (ELA) has announced that it is establishing a launch site in East Arnhem Land, on the northern coast of the Australian continent ([Space Connect](#)). The company has been granted a lease from traditional owners of a 60-hectare parcel of land near Nhulunbuy in the Northern Territory. The Arnhem Space Centre project will include multiple launch sites using a variety of launch vehicles to provide suborbital and orbital access to space for commercial, research,

and government organizations. The company recently signed an agreement with a US-based company with 25 years' experience working on space launch initiatives with NASA ([Australian Defence Magazine](#)).

## **Southern Launch**

Southern Launch is a company based in South Australia aiming to provide polar earth orbit space launch capabilities ([Southern Launch](#)). It also aims to research and implement new and novel space launch vehicle guidance and control algorithms on flight hardware for customers ([Southern Australian Space Industry Centre](#)). It has announced plans for “unhindered southward launch trajectories across unpopulated areas with low density air and nautical traffic lanes” from the Whalers Way Launch Complex on the southern tip of Eyre Peninsula in South Australia ([Southern Launch](#)).

## **Gilmour Space Launch Services**

Gilmour is an Australian launch provider whose stated aim is to develop and launch low-cost hybrid rockets for the fast-growing global small satellite industry ([Gilmour Space](#)). It has developed and tested a hybrid rocket engine and is about to conduct a series of suborbital test flights from Queensland as the next stage of its ultimate plan to provide commercial launch services from Australia. A recent report commissioned by the Government of Queensland pointed to unique opportunities for space systems, launch activities, and ground systems in Queensland ([Deloitte](#)).

## **Other Initiatives**

- From 2014 to 2019, the Space Environment Research Centre (SERC), comprising participants from the Australian National University and RMIT University; industry partners – EOS Space Systems, Lockheed Martin, and Optus Satellite Networks; and public sector research agency, the Japanese National Institute of Information and Communications Technology, carried out a successful R&D program building on Australian expertise in the measurement, monitoring, analysis, and management of space debris in order to develop new technologies and strategies to preserve the space environment. SERC's research programs were designed to build on world-leading Australian innovations to reduce and ultimately prevent the loss of space infrastructure due to collisions between debris and satellites. Its two research objectives were to establish more efficient and effective space debris collision avoidance for active satellites by providing significant improvements in predicting the orbits of debris, allowing active satellites to maneuver in time and to maneuver space debris away from collisions using lasers on the earth. Its research outcomes included developing passive and active track sensors, development of adaptive optics astrometry capabilities, and development of high-power lasers and phased laser beam combining.

- In May 2016 the Australian Department of Defence announced that it is preparing a roadmap for a \$2.3 billion next-generation satellite communications capability. The project was planned including a mix of commercial and military satcom capability. It was expected that around \$2.2–2.3 billion would be allocated over the next decade for the joint project.
- In October 2016 the Australian Minister for Defence announced that the Defence Department had commenced a research program using miniature satellites in support of Defence radar capabilities and to conduct scientific experiments. Space mission “Buccaneer” was a partnership between Defence Science and Technology (DST) and the University of New South Wales to conduct calibration activities for the Jindalee Operational Radar Network (JORN) as well as undertake outer atmosphere characterization experiments.
- In June 2017 the Australian Government announced a \$500 million investment to improve Australia’s space-based intelligence, surveillance, and reconnaissance capabilities “to support ADF operations around the world and at home to secure our borders ([Australian Government, Department of Defence](#)).” Known as Defence Project 799, the specific aim was to enhance Australia’s geospatial intelligence capabilities. The announcement said that Phase 1 of the project would provide Australia with direct and more timely access to commercial imaging satellites to support a wide range of Defence and national security activities.
- In April 2019 the Australian Government in conjunction with the Australian Space Agency laid out a 10-year roadmap for the country’s space sector. The new strategy will be backed by an AUD 19.5 million national Space Infrastructure Fund to support Australia’s domestic space industry. The Australian Civil Space Strategy 2019–2028 will have a staged focus across seven national priority areas. Those areas are position, navigation, and timing; earth observation, communication technologies, and services; “leapfrog” R&D; space situational awareness; robotics and automation; and access to space. Australian Government agency Geoscience Australia had previously received AUD 224.9 million for the space-based augmentation positioning initiative and AUD 36.9 million for the Digital Earth program. The period from 2021 to 2028 will focus on the remaining four priorities of leapfrog R&D, space situational awareness, robotics and automation, and access to space.
- In April 2019 the Australian Government announced AUD 55 million funding under its Cooperative Research Centres Program for a new industry and university R&D program, called the SmartSat CRC ([Australian Government, Business, Cooperative Research Centres](#)). The mission of the SmartSat CRC will be to foster the creation of next-generation space technologies and make Australia more competitive in the global space economy by supporting the next wave of growth in critical industries including agriculture, transport, logistics, communications, and mining, generating new hi-tech jobs and strengthening national defence and security. Over 90 companies, research institutions and government agencies, including the Australian Government Defence Science and Technology Group, will participate in the AUD 245 million 7-year program.

## Conclusion

After decades of wavering government support for the space sector in Australia, there are signs that a coherent public program of capability development and R&D support, commensurate with Australia's strategic and social needs, is emerging. The programs and initiatives outlined in this chapter are driven in part by a greater understanding of the national security dependencies and risks that Australia as a nation is exposed to and provide evidence that Australia is now treating space as an integral component of its role in the protection of its national security interests and in the advancement of its international responsibilities.

---

## References

- Australian Defence Magazine, Space launch site for Australia wins US deal, 5 February 2019. <https://www.australiandefence.com.au/news/space-launch-site-for-australia-wins-us-deal>
- Australian Government, Business, Cooperative Research Centres (CRC) Grants, CRC selection round outcomes. <https://www.business.gov.au/assistance/cooperative-research-centres-programme/cooperative-research-centres-crcs-grants/current-crc-selection-round>
- Australian Government, Department of Defence, 2016 Integrated Investment Program, 25 February 2016. <http://www.defence.gov.au/WhitePaper/Docs/2016-Defence-Integrated-Investment-Program.pdf>
- Australian Government, Department of Defence, 2016 Defence White Paper, 25 February 2016. <http://www.defence.gov.au/WhitePaper/>
- Australian Government, Department of Defence, The Hon Christopher Pyne MP (former Minister for Defence Industry), \$500 million for enhanced satellite capability, Media Release 18 June 2017. <https://www.minister.defence.gov.au/minister/christopher-pyne/media-releases/500-million-enhanced-satellite-capability>
- Australian Government, Department of Defence, 2018 Defence Industrial Capability Plan, 23 April 2018. <http://www.defence.gov.au/SPI/Industry/CapabilityPlan/Docs/DefenceIndustrialCapabilityPlan-web.pdf>
- Australian Strategic Policy Institute, The Strategist, Peter Jennings, Australia's future in space – building Australia's strategy for space, 14 June 2018. <https://www.aspistrategist.org.au/australias-future-in-space/>
- Australian Strategic Policy Institute, The Strategist, Richard Harrison, Building the rewards of space – building Australia's strategy for space, 8 June 2018. <https://www.aspistrategist.org.au/balancing-the-risks-and-rewards-of-space/>
- Australian Strategic Policy Institute, The Strategist, Malcolm Davis, Australia's space future: where to next on the final frontier? – Building Australia's strategy for space, 23 May 2018. <https://www.aspistrategist.org.au/australias-space-future-where-to-next-on-the-final-frontier/>
- Australian Strategic Policy Institute, The Strategist, Greg Rowlands, A capability conflux: on military space, cyber & autonomous modernisation – building Australia's Strategy for Space, 23 May 2018. <https://www.aspistrategist.org.au/a-capability-conflux-on-military-space-cyber-autonomous-modernisation/>
- Deloitte, Sky is not the limit: building Queensland's space economy, 24 February 2019. <http://www.dsdmip.qld.gov.au/resources/report/space/building-qld-s-space-economy.pdf>
- Gilmour Space. <https://www.gspacetech.com/>
- Review of Australia's Space Industry Capability. – report from the Expert Reference Group for the review, 29 March 2018. [https://www.industry.gov.au/sites/g/files/net3906/f/June%202018/document/pdf/review\\_of\\_australias\\_space\\_industry\\_capability\\_-\\_report\\_from\\_the\\_expert\\_reference\\_group.pdf](https://www.industry.gov.au/sites/g/files/net3906/f/June%202018/document/pdf/review_of_australias_space_industry_capability_-_report_from_the_expert_reference_group.pdf) at p.68

- Southern Australian Space Industry Centre. <https://www.sasic.sa.gov.au/industry-and-grants/capability-directory/southern-launch>
- Southern Launch. <https://southernlaunch.space/>
- Southern Launch. <https://southernlaunch.space/whalers-way>
- Space Connect, NT launch sites one step closer to reality, 4 December 2018. <https://www.spaceconnectonline.com.au/launch/3109-nt-launch-sites-one-step-closer-to-reality>
- Space Industry Association of Australia, SIAA White Paper, Advancing Australia in Space, 21 March 2017. <https://www.spaceindustry.com.au/wp-content/uploads/2019/04/SIAA-White-Paper-Advancing-Australia-in-Space.pdf>
- Space News, Australia to establish national space agency, 24 September 2017. <https://spacenews.com/australia-to-establish-national-space-agency/>



Ahmad Khan, Tanzeela Khalil, and Irteza Imam

## Contents

Introduction .....	1456
Pakistan's Space Program .....	1456
Pakistan's National Space Agency .....	1456
Historical Milestones in Space by Pakistan .....	1457
Space Budget .....	1458
Space Infrastructure in Pakistan .....	1460
Ground Station Network .....	1460
Space Sector Infrastructure .....	1460
Space Educational Institutions .....	1460
Pakistan's Space Security and Governance .....	1461
Pakistan's Space Strategic Priorities: Socioeconomic Benefits .....	1464
International Cooperation .....	1466
Pakistan's Space Vision 2047 .....	1467
Challenges Ahead and Concluding Remarks .....	1468
References .....	1468

## Abstract

Despite political, technological, and economic constraints, Pakistan is considered an aspiring space power with a relatively modest space program compared to the larger, more successful Asian ones of China and India. Innovative leadership, smart allocation of national resources, and political will are all necessary for any

A. Khan (✉)

Department of Strategic Studies, National Defence University, Islamabad, Pakistan  
e-mail: [ahmad\\_ishaq669@yahoo.com](mailto:ahmad_ishaq669@yahoo.com)

T. Khalil

South Asia Center, Atlantic Council, Washington, DC, USA  
e-mail: [tanzeela\\_khalil@hotmail.com](mailto:tanzeela_khalil@hotmail.com)

I. Imam

Department of Defence and Strategic Studies, Quaid-i-Azam University, Islamabad, Pakistan  
e-mail: [irttyza@gmail.com](mailto:irttyza@gmail.com)

country to progress in such a high-technology field. Pakistan can utilize available resources to improve its nascent space infrastructure through collaborative efforts to gain eventual self-sufficiency for socioeconomic and strategic purposes in the South Asian region. Since its inception, space activities remained slow; however, there were substantial milestones achieved by Pakistan in space primarily for socioeconomic benefits. Likewise, Pakistan supports multilateral agreements to prevent the weaponization of space and has ratified all United Nations space treaties. Furthermore, multilateral collaboration, the utilization of available resources and public-private partnerships empowering its space program, enhances its domestic scientific and technological base and builds an indigenous space industry that can reap dividends at home and abroad. This can also benefit Pakistan's needs to mainstream its national space program for the overall national growth of the country and meet future requirements.

---

## Introduction

On October 25, 2018, the then Minister for Information and Broadcasting, Chaudhry Fawad Hussain, declared, in a press conference after a cabinet session of the Federal Government of Pakistan, the country's intention for a first space mission by 2022 (Pakistan to Launch First Space Mission in 2022 2018). The former Information Minister announced that a Memorandum of Understanding (MOU) had been signed between a Chinese company and Pakistan's main space agency, the Space and Upper Atmosphere Research Commission (SUPARCO), for a joint manned space venture. This announcement came not only in the wake of Pakistan's recent satellite launches, of the Pakistan Remote Sensing Satellite (PRSS)-1 and the Pakistan Technology Evaluation Satellite (PakTES)-1A by China in July 2018 (Siddiqui 2018), but also in the context of Pakistan's neighboring rival, India, and its ambitious space missions (Ahsan and Khan 2019). Unlike the well-established Chinese and Indian space programs for both civilian and military purposes, Pakistan's space odyssey has been slow in keeping pace with the rest of the world due to a myriad of reasons. These range from an inadequate scientific and technological base, mostly due to technological denial from the Western countries that could propel an indigenous space program on its own (Ahsan and Khan 2019).

---

## Pakistan's Space Program

### Pakistan's National Space Agency

Soon after the prolific launch of Soviet Union's first artificial satellite, Sputnik 1, Pakistan started pursuing a space program to join the race of grasping the enormous advantages of outer space research and exploitation. The Space and Upper Atmosphere Research Commission (SUPARCO), the official space agency of the

Government of Pakistan, is in charge of the country's civil and public space program SUPARCO. Pakistan's premier space agency was established through a presidential ordinance in 1981 and its charter was approved by the National Assembly of Pakistan in 1987 during President Zia-ul-Haq's regime (1977–1988). SUPARCO is the successor to the Pakistan Space and Upper Atmosphere Research Committee, which was founded in September 1961. This committee was part of the Pakistan Atomic Energy Commission (PAEC) before becoming a separate organization in 1964. The committee was instrumental in developing and testing its Rehbar sounding rockets with support from the US National Aeronautics and Space Administration (NASA), the British National Space Centre (BNSC), and the French Centre National d'Etudes Spatiales (CNES), as well as numerous Western aerospace companies. All the major milestones achieved by Pakistan in space odyssey are due to SUPARCO (Mehmud 1989).

Since its inception in the 1960s, SUPARCO gradually expanded into satellite technology in the 1970s in the fields of remote sensing, imagery, telecommunication, atmospheric testing, and other scientific measurements, while it provided technical training and employment for its ground-based satellite stations across the country. SUPARCO continued its scientific outreach with its counterparts worldwide and was the country's main participant in numerous scientific treaties and international agreements in the United Nations (UN) and other organizations. Due to the strategic nature of space, SUPARCO, since 2000, falls under the Strategic Plans Division (SPD) umbrella of Pakistan, which is the operating arm of the country's National Command Authority (NCA). The other stakeholders partially associated with the space program are the Pakistan Telecommunication Authority (PTA), the Frequency Allocation Board (FAB), the Ministry of Information Technology (MoIT), and the Ministry of Science and Technology (Mehmud 1989).

## Historical Milestones in Space by Pakistan

Pakistan's aspiration to acquire space technology can be traced back to the late 1950s. The establishment of SUPARCO in 1961 was the first step towards space exploration and space technology. Due to the lack of adequate resources and technologies, Pakistan's space program aimed at peaceful uses through the development of civilian space applications. The objectives of Pakistan's space program have largely remained confined to human resource development, telemedicines, remote sensing and geographic information system (GIS), communication satellites, and peaceful uses of outer space through support to the UN and other nation's agenda for peaceful uses of space and preventions of an arms race in outer space.

Pakistan has launched six space objects, namely are BADR-1, BADR-2, PAKSAT-1, ICUBE-1, PRSS-1, and PakTES-1A launched in 1990, 2001, 2011, 2013, and 2018 respectively. BADR-1 was launched to "test and validate the indigenously developed satellite subsystems in the space environment." In addition to this, the BADR-1 satellite was also aimed to gather real-time voice and data communications experiments between two ground systems in the ultra and very



high-frequency bands. BADR-1 was launched through a Chinese rocket carrier Long March 2E. On December 10, 2001, Pakistan launched its second satellite BADR-B in space. The general function of BADR-B aimed to “acquire data on space weather” and mapping carbon and other earth resources in different parts of Pakistan. BADR-B was launched from the Baikonur Cosmodrome in Kazakhstan with the cooperation of ROSCOMOS, Russian Space Agency, through its Zenit carrier rocket. BADR-B was Pakistan’s first remote sensing satellite. Pakistan’s third and most successful satellite, PAKSAT-IR, was launched on August 12, 2011. It was Pakistan’s first communication satellite in space exported from China. PAKSAT-IR was launched from Xichang Satellite Launch Centre through the Long March 3B rocket, and primarily it is a telecommunication satellite on which more than half of the country’s TV channels are linked and broadcasting their services. Pakistan’s latest space objects launched were PRSS-1 and PAKTES-1A using Long March 2C rocket (Mehdi and Su 2019).

Pakistan’s acquisition of communication satellite PAKSAT-IR played a significant role in various areas of development in Pakistan. It helped Pakistan to expand its communication infrastructure to not just urban but rural areas as well. It enhanced the overall connectivity in the country as it became the preferred choice for leading mobile companies (Mehdi and Su 2019).

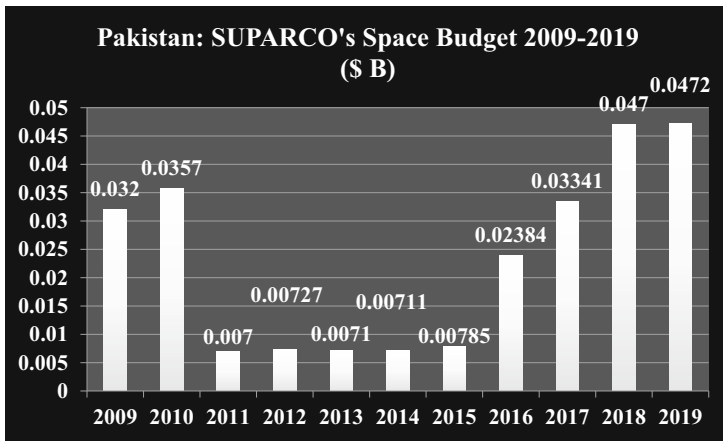
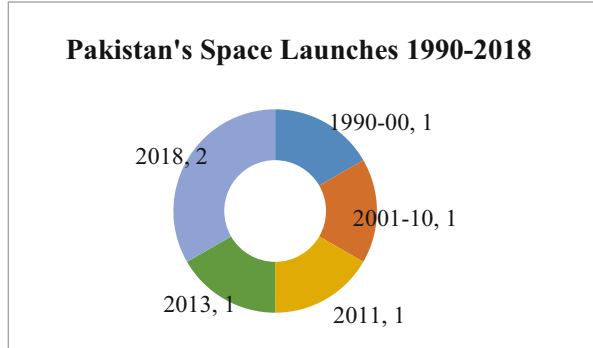
Launch of communication satellite PAKSAT-1R from Xichang Satellite Launch Centre into GEO is marked as the defining moment in Pakistan’s space program. It replaced PAKSAT-1 and is capable of providing telecommunications and broadcast services to Pakistan. It is fitted with 12 active C-band and 18 active Ku-band transponders. The service life span of the satellite will be 15 years (Mehdi and Su 2019).

In 2016, SUPARCO and China Great Wall Industry Cooperation (CGWIC) signed an agreement for the development and launch of the Pakistan Remote Sensing System (PRSS-1). PRSS-1 was designed and built by China for Pakistan, as its first active Earth observation satellite. In July 2018, PRSS-1 and indigenously produced Pakistan Technology Evaluation Satellite (PAKTES-1A) were launched together on board Long March 2C launch vehicle from Jiuquan Satellite Launch Center. PAKTES-1A remote sensing satellite has, consequently, represented the foundation of Pakistan’s capability to launch its domestically build remote sensing satellite (Mehdi and Su 2019) (Fig. 1).

## Space Budget

Pakistan’s space program has modest financial resources to augment full-fledged space exploration activities. SUPARCO is the premier space agency in Pakistan and is primarily responsible for manufacturing, developing, and launching space objectives and other associated technologies. SUPARCO’s financial support from the government remained little. SUPARCO was established in 1961 as a space science research wing of Pakistan Atomic Energy Commission (PAEC) (Moltz 2012). PAEC

**Fig. 1** Pakistan's space launches. (Source: Mehdi and Su 2019)



**Fig. 2** SUPARCO's space budget. (Source: Pakistan Economic Survey 2009-2019)

was established in March 1956, 5 years before the establishment of SUPARCO. However, PAEC got the attention of the policymakers as it was thought that nuclear program was suitable for the socio-economic and national security purposes. Since its establishment in 1956, PAEC has now become a huge enterprise in Pakistan, serving in different fields and many corners of life including research and development (R&D), and in agriculture, industry, health sector. In the early 2000s, former President General Pervez Musharraf increased the financial budget of SUPARCO, breaking its financial stalemate. However, it is safe to say that it is still not sufficient enough to carry out an extensive space program including manufacturing its satellite indigenously and launching it from its soil. Pakistan has no dedicated launch pad for its SLVs, neither has its rocket to send satellites into space. To build an SLV and a launching pad, SUPARCO requires a tenfold budget increment for at least next 5 years. The figure shows SUPARCO's financial allocations to carry out its activities from 2009 to 2019 (Fig. 2).

## Space Infrastructure in Pakistan

### Ground Station Network

There are three satellite ground stations in Pakistan, located in Lahore, Islamabad, and Karachi. The ground station facility of Islamabad was developed in the 1970s and equipped with the Landsat and SPOT satellite ground receiving antennae. The remote sensing data processing facility was also established to process the raw data. The GCS for PRSS-1 satellite was established in the same facility in 2018 for TT&C and data reception. The ground station at Lahore was established in 2010 to control and operate the Paksat-1R satellite. This ground station is equipped to perform the telemetry, tracking, and control facility. The satellite ground station at Karachi was established in 2010, to perform the functions of backup station of Lahore station for Paksat-1R TT&C and operations.

### Space Sector Infrastructure

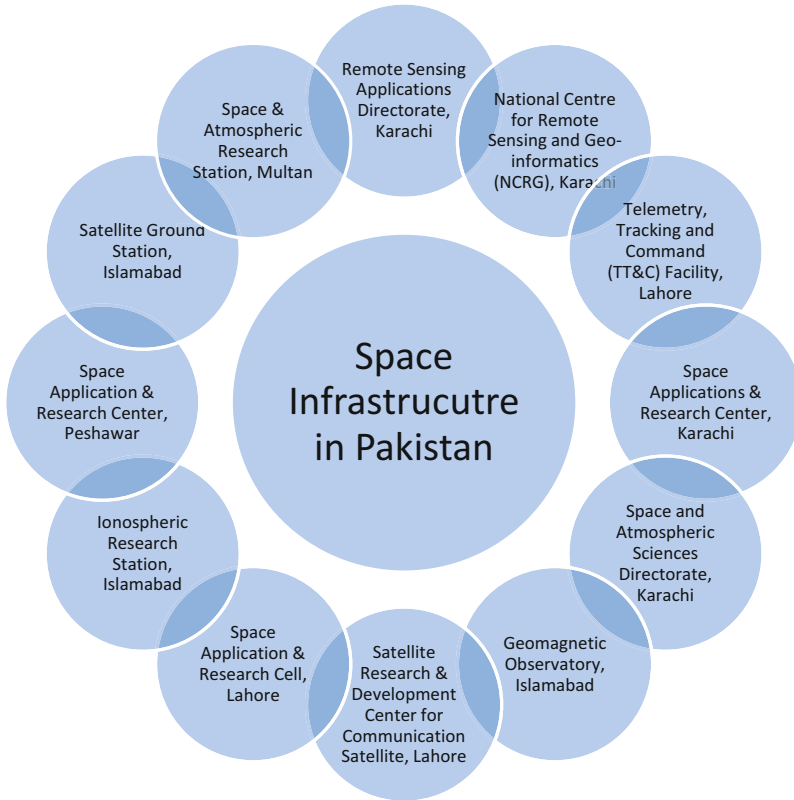
Overall, Pakistan has established the following facilities related to the space sector as seen in Fig. 3 below.

### Space Educational Institutions

Space education is the backbone of the Pakistan space program. There are three major space educational institutes in Pakistan providing necessary education in space applications and technological development in Pakistan. These three institutions include the Institute of Space Technology (IST) in Islamabad, the Department of Space at the University of Punjab, and the Institute of Space Science and Technology at the University of Karachi. All these institutes and departments are providing a pool of space scientists to foster Pakistan's space program. These institutes provide education at graduate, postgraduate, and PhD level in space science to foster the necessary pool of scientists in Pakistan.

The IST is the largest space education institute in Pakistan. The university was established in 2002 to solidify space science in Pakistan. It offers undergraduate and postgraduate degrees in aerospace engineering and communication systems engineering as its core discipline (About IST 2020). The department of space is the pioneer space education department in Pakistan. The University of Punjab, Lahore, established the department in 1985. The department was established to meet the rapid development in the field of space exploration, the subject of space science, telecommunications, meteorology, and related fields (Department of Space Science 2020).

The Institute of Space Science and Technology aims to achieve excellence in space science and associated technologies to bolster Pakistan's space program. The institute is the finest in Pakistan to deal with aerospace engineering. The curriculum



**Fig. 3** Space infrastructure in Pakistan. (Source: Introduction-Facilities 2020)

offered to undergraduate and postgraduate students is designed to comply with international standards, emerging technologies, and to meet the indigenous requirements of Pakistan in space exploration (Introduction 2020).

---

## Pakistan's Space Security and Governance

Pakistan has ratified all UN space treaties and is a party to one space-related treaty, one agreement, one convention, and one organization (see Table 1 for details). Among others, Pakistan has also supported the International Code of Conduct (ICoC). Also in 2014, the UN General Assembly adopted a Russian resolution titled "No First Placement of Weapons in Outer Space." The resolution calls for a nonbinding restriction against the first placement of weapons in outer space. The United States and other like-minded states are against the adopted resolution.

**Table 1** Pakistan's participation to UN outer space treaties, international agreements, and organizations. (Source: UNCOPUOS 2020)

Treaties, conventions, agreements, organizations	UN treaties				Space related treaty, agreements, and organizations											
	OST	ARRA	LIAB	REG	MOON	NTB	BRS	ITSO	INTR	ESA	ARB	INTC	IMSO	EUTL	EUM	ITU
<b>Pakistan</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	<b>R</b>	-	<b>R</b>	-	-	-	-	<b>R</b>	-	-	<b>R</b>

Pakistan and Russia, on the sidelines of Shanghai Cooperation Organisation (SCO) in 2019, signed a joint statement on the initiative with Russia (Khan and Sadeh 2019).

Additionally, Pakistan has been a tough proponent of disarmament and arms controls treaties. Over the years, various statements and resolutions flooded by Pakistani diplomats at various international disarmament *fora* such as the UN First Committee, Conference on Disarmament (CD), etc., have called for arms control, limitation, prevention of space weaponization, and disarmament agreements at both bilateral and multilateral levels. Pakistan has been a proponent and advocate of the notion that space should be a global commons and should not be weaponized. If one observes the various official statements and resolutions tabled by Pakistan on UN governed arms control and disarmament forums such as the UN First Committee (DISEC), the CD, and UN Fourth Committee, there is a pattern that Pakistan has always been cognizant of the threats to the world peace that emanate from the militarization and weaponization of space. Pakistan has also supported the establishment of the Group of Governmental Experts (GGE) in CD to prepared expert-level recommendations to negotiate a treaty to prevent the weaponization of space and maintain the long term sustainability of activities in outer space (Khan and Khan 2019). In 2016, the then Pakistan Permanent representative in CD, Ambassador Tehmina Janjua, who later became the Foreign Secretary stated that “outer space is the common heritage of all humankind. It is in the collective interest to explore and use outer space exclusively for peaceful purposes, for the benefit of all. It should not be militarized or weaponized and turned into a realm of conflict” (Janjua 2016). She further expressed that “Weaponization of outer space is not science fiction anymore. With the ever-growing use of outer space by an increasing number of states, both for civilian and military purposes, the potential and the risk of its weaponization cannot be ruled out. Weapons in space would lead to instability, and negatively affect international and regional peace and security” (Janjua 2016).

As far as the Outer Space Treaty (OST) is concerned, Pakistan recognized that the exploration and use of outer space shall be carried out for the benefit and in the interests of all countries and shall be the province of all humanity. Pakistan endorses that the OST prohibits the placement of nuclear weapons and other weapons of mass destruction in outer space. However, Pakistan believes that there is a need to recollect thoughts on the placement of other types of weapons including conventional weapons in outer space to make space safer and sustainable (► Chap. 3, “Challenges to International Space Governance”). Pakistan considers that all of these concerns need to be addressed in a legally binding treaty, which is universally accepted. Pakistan is arguing for several decades in favor of developing long term sustainable guidelines for spacefaring nations to conduct peaceful activities in space. Pakistan is cognizant of the fact that the international community has continued to make efforts to prevent the weaponization of space. Pakistan has welcomed various proposals in the General Assembly which aim to address the weaponization of space with overwhelming support (Khan and Khan 2015).

The above quoted statement by Pakistan's Permanent Representative to the United Nations and CD is just one example of Pakistan's stance and commitment

towards the goals set out by the idea of Prevention of an Arms Race in Space (PAROS). From the above quoted statement, Pakistan's threat perception can be seen as one of the factors driving the country's interest for a solid, effective, all-encompassing, and legally binding instrument.

Likewise, Pakistan is a proactive member of the UN Office for Outer Space Affairs (UNOOSA), Committee on Space Research (COSPAR), the UN Committee on the Peaceful Uses of Outer Space (UNCOPUOS), CD, and other multilateral forums for space security and governance (see Table 2 for details).

---

## **Pakistan's Space Strategic Priorities: Socioeconomic Benefits**

The peaceful application of space capability and technology can bring about viable socioeconomic development and enhance the standards of living for the citizens of Pakistan. For instance, a communication satellite system is considered as the best service provider for teleeducation, telemedicine and channels in remote areas. Remote sensing satellites can contribute to discovering solutions for water management, land management, food security, disaster management, urban planning, and resource exploration. The PRSS-1 is a game-changer for Pakistan's space program. Remote sensing satellites can play an instrumental role in reducing the chances of intra-state conflict by providing adequate and well-informed data to deal with nontraditional threats like water scarcity and food shortage. Navigation provides free and reliable positioning on a worldwide basis. It also includes land surveying, tracking and surveillance, scientific study of earthquakes, disaster relief, and emergency services (Ahsan and Khan 2019).

Pakistan's PRSS-1 and PAKTES-1A are the result of collaboration with China. PRSS-1 was purchased from China and was originally built by the China Academy of Space Technology (CAST). PAKTES-1A was indigenously built by Pakistan. Since Pakistan does not have its dedicated launching facility, a Chinese Long March rocket was used to send both satellites to LEO. The primary aim of the satellites was to understand and enhance socioeconomic benefits of remote sensing systems. Another objective of sending these remote sensing satellites was to get continuous and improved data for the socioeconomic benefits, as both PRSS-1 and PAKTES-1A are Pakistan's first remote sensing satellites (Ahsan and Khan 2019).

Pakistan is extremely vulnerable to climate change in South Asia, despite being the lowest contributor to carbon emissions in the region. For example, historic floods during rainy seasons recently have hit the country, causing economic and human losses. Remote sensing satellites are necessary to monitor these climatic changes caused by natural and human activities. Likewise, Pakistan suffers from an acute shortage of freshwater. It is predicted that Pakistan will face water scarcity in the year 2025; this is a major issue for the country's national security and survival. Experts state that lack of access to water and food causes "social unrest and political

**Table 2** Pakistan's participation to UN bodies for space governance. (Source: websites of these organizations)

	Multilateral forums for space governance	Agenda items	Pakistan's position
1	First Committee of the UNGA – Disarmament and International Security Committee (DISEC)	Arms control and disarmament issues in outer space	Pakistan is an active member of the First Committee of the UNGA – DISEC
2	UN Committee on the Peaceful Uses of Outer Space (UNCOPUOS)	UNCOPUOS was established in 1959 to govern the exploration and use of space for the benefit of all humanity: for peace, security, and development	Pakistan is a member of UNCOPUOS since 1973
	<b>Standing committees</b> <b>(a)</b> Scientific and Technical Subcommittee (working group on the long-term sustainability of outer space activities)	The committee discusses questions related to the scientific and technical aspects of space activities	Pakistan participates actively in the proceedings of the Scientific and Technical Subcommittee
	<b>(b)</b> Legal Subcommittee	Topics include the status and application of the five United Nations treaties on outer space, the definition and delimitation of outer space, national space legislation, legal mechanisms relating to space debris mitigation, and international mechanisms for cooperation in the peaceful exploration and use of outer space	Pakistan participates actively in the proceedings of the Legal Subcommittee
3	International Telecommunication Union (ITU)	Promotes international cooperation in assigning satellite orbits, works to improve telecommunication infrastructure in the developing world	Pakistan is a member of the ITU
4	Conference on Disarmament (CD)	Proposed Prevention of an Arms Race in Space (PAROS) Treaty is one of the core issues in the permanent agenda items of the UN disarmament body	Pakistan is a member of CD. Pakistan in CD has repeatedly asked the member states to start negotiations on the PAROS treaty. Pakistan has endorsed the joint draft treaty proposal of Russia and China in CD



instability in any country.” Recently, decreased access to water and food has stirred social and economic unrest in the Middle East and North Africa. Although Pakistan has not witnessed any kind of social and economic unrest similar to those of the Middle East and North Africa, these natural resource challenges must be dealt with adequately to mitigate intrastate conflict in Pakistan. To meet this challenge, Pakistan needs to build more remote sensing capabilities to improve knowledge of its freshwater supply, drainage system, and reservoirs. Water management has historically been inadequate in Pakistan, which also hampers the country’s most significant economic sector – agriculture (Ahsan and Khan 2019).

In the wake of current nontraditional security challenges facing Pakistan, the PRSS-I has ensured Pakistan to deal with them more effectively. Remote sensing capability will prove to be beneficial for addressing the peculiar challenges of water scarcity, food shortage, and climate change. Remote sensing can also help advance the understanding in the dynamics of water quantity and quality that can be used to simulate water resources management scenarios under different water quantity or quality demands. Remote sensing can also enhance the capacity of the departments and institutions related to water management in Pakistan for better evaluation of the situation and make effective strategies to deal with the imminent crisis. Furthermore, utilization of PRSS-I data, including climate forecasting to track weather-related natural disasters like floods, storms, rain, can eventually help the accelerating response, recovery, and rebuilding efforts by the relief departments. These technologies not only provide cost efficient and effective methods of water management but they also accurately monitor and predict long term trends of depletion of resources. It is high time that SUPARCO, the Ministry of Defense, and the Ministry of Science and Technology synergized their efforts to deal with these nontraditional challenges in a more cost effective manner by utilizing the available space applications. In this regard, the Government of Pakistan should also regulate and release adequate funds for the relevant ministries and commissions. The application of space technology in various domains will also help improve the economic condition of the country.

## International Cooperation

Pakistan has established strong international collaborations. Pakistan is a permanent member of many international organizations, scientific committees, and United Nations bodies in conducting joint programs of research and development, trainings, and space research activities. Pakistan is collaborating with the following organizations/committees, where SUPARCO is its representative:

- Asia-Oceania Space Weather Alliance (AOSWA)
- Inter-Program Coordination Team on Space Weather (ICTSW)
- University of Massachusetts Center for Atmospheric Research (UMLCAR)
- Royal Meteorological Institute (RMI) – British Geological Survey (BGS)
- Institute of Tibetan Plateau Research (ITP), Chinese Academy of Sciences (CAS)
- European Commission (EC)

- Food and Agriculture Organization (FAO)
- United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS)
- United Nations Economic and Social Commission for Asia and the Pacific (UNESCAP)
- Committee on Space Research (COSPAR)
- International Society for Photogrammetry and Remote Sensing (ISPRS)
- National Coordination Committee for COSPAS-SARSAT (Search & Rescue Satellite Aided Tracking System)
- American Institute of Aeronautics and Astronautics (AIAA)
- International Astronomical Federation (IAF) and International Academy of Astronautics (IAA)
- Asian Association on Remote Sensing (AARS)
- Asia-Pacific Space Cooperation Organization (APSCO)
- Inter-Islamic Network on Space Sciences and Technology (ISNET)

---

## **Pakistan's Space Vision 2047**

Pakistan's Space Vision 2047 states that it needs information and data for planning, managing, and monitoring its natural resources in order to improve the quality of life across the country. The "Space Vision 2047" has envisioned an adequate deployment of remote sensing constellations in the future to reduce the chances of intra-state conflict over water and food shortages. This challenge also includes mapping and surveying of irrigated areas and proper estimates of crop yield, according to the previously mentioned challenges affecting Pakistan's agriculture sector. Also, the Space Vision 2047 maps commercial and private utilization of data from remote sensing satellites to foster economic growth. Pakistan has a humble space program that is designed to help the country better manage its landscape and deal with the rising challenges of climate change, as well as better manage the socio-economic potential of the country (Ahsan and Khan 2019). Pakistan has recently launched two satellites for remote sensing, imaging, and data collection. The Government aims to utilize these space assets to formulate strategies and mechanisms to mitigate the various environmental challenges such as water scarcity and water management. This vision outlines the following aims/goals:

- (a) Launching five satellites into orbit for communication purposes. The plan envisions multiband, multifrequency communication satellites that would enable Pakistan to provide wireless communication solutions to far-flung, geographically isolated areas.
- (b) Six Low Earth Orbit satellites for navigational, remote sensing, and geographic information system (GIS).
- (c) Telemedicine: In this project, various hospitals of high standards will be connected to the less developed areas of Pakistan to ensure the quality treatment of the poor and needy patients.

- (d) Teleeducation: This program includes broadcasting the educational materials of various universities to the students free of cost.

---

## Challenges Ahead and Concluding Remarks

Pakistan's space program is focused on peaceful uses of outer space in achieving economic benefits for national growth. However, Pakistan's space program has insufficient budget allocations to realize the stated goals and objectives. It is not currently in a good position to develop its own commercial space technologies and therefore faces challenges in its ability to develop dual-use space assets. It will likely take decades of work in areas from education and domestic economic reform to foreign investment policies in order to create the preconditions needed to enable Pakistan to produce its own space technologies. In the interim, Pakistan will have to try to broaden its technological base through participation in the Asia-Pacific Space Cooperation Organization (APSCO) and the Asia-Pacific Regional Space Agency Forum (APRSAF), as well as to develop domestic policies to stimulate young people to study in space-related fields (Ahsan and Khan 2019).

Pakistan is an important regional player in South Asia, with significant nuclear capability. Given that its journey into space has been largely peaceful with a focus on civilian activities, Pakistan is viewed as a responsible aspiring space actor. However, the world is witnessing an era where states are cooperating and competing in land, sea, air, and space. The major space farers – the United States, Russia, and China – see their space assets as crucial for their national growth, as well as for their national security. India has been following the example of all major spacefaring states, and it has a space program with a political priority. India sees its space program as instrumental for national growth and for national security. Even though these developments posit security challenges for Pakistan, Pakistan is currently utilizing its partnership in space with China to address challenges of climate change, and water and agricultural management, by making use of space systems and applications (Ahsan and Khan 2019). Currently, Pakistan is neither capable nor inclined to militarize and weaponize outer space, despite Chinese and Indian advances in these areas. In the future, however, Pakistan can certainly achieve credible options for military uses of space assets if this is warranted and in line with the space treaties.

---

## References

- About IST: Overview (2020) Institute of Space Technology. <http://www.ist.edu.pk/about>. Accessed 9 Mar 2020
- Ahsan A, Khan A (2019) Pakistan's journey into space. *Astropolitics* 17(1: Special issue on Space Power and Security Trilemma in South Asia):38–50
- Department of Space Science (2020) The University of Punjab. <http://pu.edu.pk/home/department/62/Department-of-Space-Science>. Accessed 9 Mar 2020
- Introduction-Facilities (2020) Pakistan Space and Upper Atmosphere Research Commission, <http://www.suparco.gov.pk/pages/intro.asp>. Accessed 27 May 2020

- Introduction: Institute of Space Science and Technology (2020) University of Karachi. [http://www.uok.edu.pk/research\\_institutes/ispa/index.php](http://www.uok.edu.pk/research_institutes/ispa/index.php). Accessed 9 Mar 2020
- Janjua T (2016) Statement by Ambassador Tehmina Janjua, permanent representative of Pakistan to the United Nations, Geneva and conference on disarmament during the thematic debate of the first committee on outer space. Pakistan Mission to United Nations
- Khan Z, Khan A (2015) Chinese capabilities as global space power. *Astropolitics* 17(2–3):185–204
- Khan Z, Khan A (2019) Space security trilemma in South Asia. *Astropolitics* 17(1: Special issue on Space Power and Security Trilemma in South Asia):4–22
- Khan A, Sadeh E (2019) Introduction: space power and security trilemma in South Asia. *Astropolitics* 17(1: Special issue on Space Power and Security Trilemma in South Asia):1–4
- Khan A, Ullah S (2020) Challenges to international space governance. In: Schrogl K et al. (Eds.) *Handbook of Space Security: Policies, Applications and Programs*. Springer, Cham
- Mehdi M, Su J (2019) Pakistan space programme and international cooperation: history and prospect. *Space Policy* 47(1):175–180
- Mehmud S (1989) Pakistan's space programme. *Space Policy* 5(3):217–226
- Moltz C (2012) *Asia's space race: national motivations, regional rivalries, and international risks*. Columbia University Press, New York
- Pakistan to Launch First Space Mission in 2022: Fawad Chaudhry (2018) *Geo News*. <https://www.geo.tv/latest/216047-pakistan-to-launch-first-space-mission-in-2022-fawad-chaudhry>. Accessed 25 Aug 2019
- Pakistan Economic Survey (2019) Ministry of Finance, Government of Pakistan, [http://www.finance.gov.pk/survey\\_1819.html](http://www.finance.gov.pk/survey_1819.html). Accessed 27 May 2020
- Siddiqui N (2018) Pakistan Launches Remote Sensing Satellite in China. *Dawn*, <https://www.dawn.com/news/1418966/pakistan-launches-remote-sensing-satellite-in-china>. Accessed 9 July 2018
- UNCOPUOS (2020) Status of international agreements relating to activities in outer space as at 1 January 2020. <https://www.unoosa.org/oosa/en/ourwork/spacelaw/treaties/status/index.html>. Accessed 29 May 2020



# Space Sector Economy and Space Programs World Wide

# 73

Per Høyland, Estelle Godard, Marta De Oliveira, and  
Christina Giannopapa

## Contents

Introduction .....	1472
The Space Sector Economy and Activities .....	1473
The Institutional Space Sector .....	1475
The Commercial Space Sector .....	1480
Forecasts for Government Space Budgets and Programs .....	1484
Conclusions .....	1496
References .....	1496

## Abstract

In the following chapter an overview of the space-related budgets is presented. This should provide a quantitative perspective of the overall market value and financial performance of the space activities of recent years. Accurate estimations of global space activities are complicated, due to nontransparent government space budgets in particular on defense-related programs and the lack of a stan-

---

P. Høyland (✉)

Department of Political Science, University of Oslo, Oslo, Norway  
e-mail: [perhoyl@uio.no](mailto:perhoyl@uio.no)

E. Godard

Institut d'études politiques de Paris, Paris, France  
e-mail: [estelle.godard@sciencespo.fr](mailto:estelle.godard@sciencespo.fr)

M. De Oliveira

International Space University (ISU), Illkirch-Graffenstaden, France  
e-mail: [marta.oliveira@community.isunet.edu](mailto:marta.oliveira@community.isunet.edu)

C. Giannopapa

European Space Agency (ESA), Paris, France  
e-mail: [christina.giannopapa@esa.int](mailto:christina.giannopapa@esa.int)

standardized approach for measuring them. A forecast for government space budgets and programs is also provided.

---

## Introduction

Space technologies and their applications are part of our everyday life. They vary from using mobile phones, watching live TV broadcasting, making banking transactions, weather forecasting, air traffic management, etc. Its use has broadened from serving a limited number of space fearing nations driven by defense objectives into a more innovation-driven community including civilian, security, and private sector communities. Even though space activities are taking place already for more than half a century, there is no unified definition of what the space sector is, let alone space security.

In spite of being characterized by an intense international cooperation, the space sector relies above all on institutional captive markets with limited room for global competition. This is an important element in a return-on-investment analysis regarding public funding. However, it should be taken into consideration that accurate estimate of global space activities is a complicated task. This is due to the lack of a standardized approach and the lack of transparency in certain government space programs, such as defense-related programs. Additionally, the publication of financial figures by commercial companies is not uniform across the sector and varies in time.

Space remains highly oriented towards the generation of scientific, social, and/or strategic returns rather than primarily an immediate source of profit in terms of commercial return, the latter nevertheless being a major concrete feature. Thus, the value of space research and development and subsequent operational assets is first of all political and considered in a long-term economic strategy, whereby institutional funding supports the inception, then the maturing of a specific domain. This is what has justified constant public investment since the dawn of the space age. In particular institutional budgets often contribute to the start-up and development of capital-intensive and high-technology sectors such as space (OECD 2016).

As confirmed by the Organization for Economic Cooperation and Development (OECD), since the beginning of the economic crisis, the space sector has fared relatively well, in part because space is a strategic sector, often supported due to national imperatives and institutional funding, because space still supports the implementation of national objectives, and thanks to the good position of telecommunications in growing mass markets (OECD 2011, p. 29). Global government space expenditures peaked in 2012 followed by declining figures, yet this trend has changed lately. Euroconsult (2019) expect to see a growth in both defense and civil spending towards 2028. The cyclical nature of the industry in replenishing satellites as well the continuing commercial successes of many space services have contributed to the dynamism of the entire value chain. This is a fundamental element for the future forecast of space in Europe insofar as space cannot be considered a “stop and go” economy, meaning that any break in public investments would result in an

immediate loss of industrial capabilities (human or otherwise) which could not be easily restarted later on.

Nowadays, a major shift in the space economy is driven by the commercial launch and satellite manufacturing industries. The market is set to grow fast due to falling costs and reduced obstacles to participate in the economy. Examples of emerging sectors in the space economy for the coming years are space tourism, asteroid mining, and in-orbit manufacturing. At the same time, exploration is brought deeper into space and existing activities related to navigation, Earth observation, and telecommunication continues to develop (ESA LTP 2017).

This chapter defines the space sector according to OECD and provides an overview of the space-related budgets worldwide. Institutional as well as commercial space activities are considered. It provides a quantitative perspective of the overall market value and financial activities over the past years complimented by a forecast of government space expenditures through 2028, as provided by Euroconsult.

---

## The Space Sector Economy and Activities

There is no unified definition of the space sector and what it includes. According to OECD (2011), the space sector has nine main product groups of high technology: (1) aerospace, (2) computers and office machines, (3) electronics and telecommunications, (4) pharmacy, (5) scientific instruments, (6) electrical machinery, (7) chemistry, (8) nonelectrical machinery, and (9) armaments (Hatzichronoglou 1997). There is no specific “space activity classification.” In the United Nations International Standard Industrial Classification (ISIC, Rev.4 released in August 2008), most parts of the space sector are included under different categories. Therefore, isolating the space sector from aerospace and defense sector remains a challenge for a number of countries.

The space sector over the years has become more commercial, and different space applications have emerged outside the traditional research and development (R&D), calling for a wider definition of space economy. This wider “space economy” can be defined using different angles. It can be defined by its products (e.g., satellites, launchers), by its services (e.g., broadcasting, imagery/data delivering), by its programmatic objectives (e.g., military, robotic space exploration, human space-flight, Earth observation, telecommunications), by its actors/value chains (from R&D actors to users), and by its impacts (e.g., direct and indirect benefits). One drawback is that narrow definitions might ignore important aspects, such as the R&D actors (e.g., labs and universities) and the role of the military (i.e., as investor in R&D budgets and a customer for space services), or ignore scientific and space exploration programs altogether (OECD 2011, p. 16).

The OECD (2016) provides the following definition of the space economy:

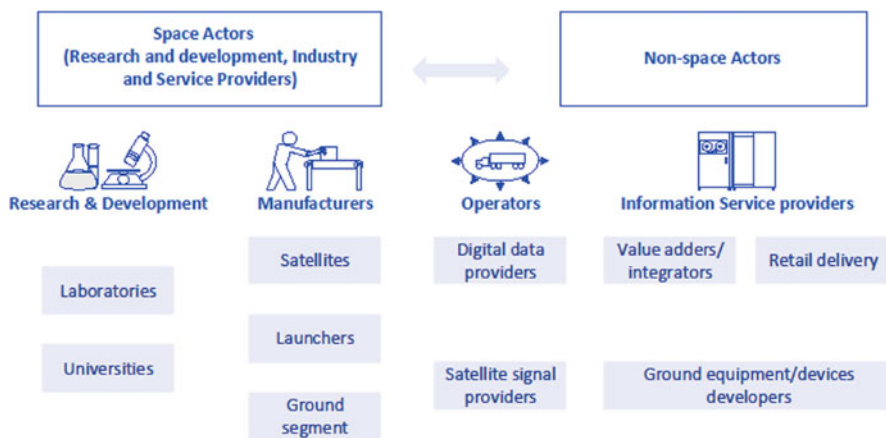
The space economy is the full range of activities and the use of resources that create and provide value and benefits to human beings in the course of exploring, understanding, managing and utilising space. Hence, it includes all public and private actors involved in developing, providing and using space-related products and services, ranging from research

and development, the manufacture and use of space infrastructure (ground stations, launch vehicles and satellites) to space-enabled applications (navigation equipment, satellite phones, meteorological services, etc.) and the scientific research generated by such activities. It follows that the space economy goes well beyond the space sector itself, since it also comprises the increasingly pervasive and continually changing impacts (both quantitative and qualitative) of space-derived products, services and knowledge on the economy and society.

The concept of “New Space” encapsulates the global trend of emerging investment philosophies and series of technological advancements stimulating a space industry largely driven by commercial motivations (EIB Advisory 2018). This wider space economy can be broken down in to three parameters (OECD 2016):

- (i) The upstream space sector covering activities related to space infrastructures, including R&D, satellite, and launchers manufacturing, and the deployment of such infrastructures
- (ii) The downstream space sector primarily related to commercial activities based on the use of data provided by space infrastructures, such as broadcasting, communication, navigation, and Earth Observation
- (iii) The space-related or derived activities in other sectors

The space economy is larger than the traditional space sector (e.g., rockets and satellites). It also involves new services and product providers (e.g., geographic information systems developers, navigation equipment sellers) which are using space system’s capacities to create new products. However, the unique capabilities offered by satellites (i.e., ubiquitous data, communications links, imagery) represent often only small, albeit essential, components of those new products and services (Fig. 1). Investments in manufacturing of satellites for earth observation, navigation, and telecommunication result tens of multiples in the downstream sector. Integrated



**Fig. 1** The space economy’s simplified value chain. (Source: OECD 2011)

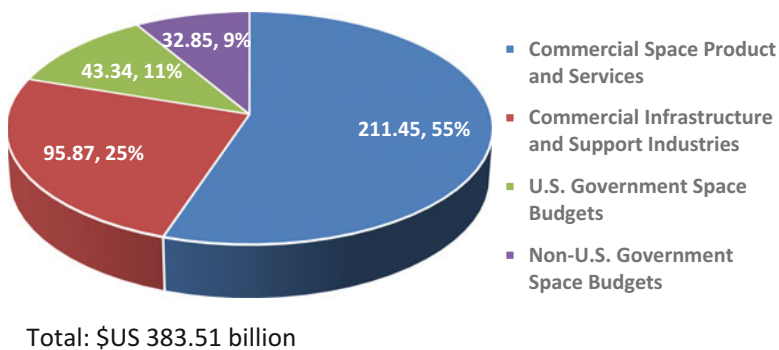


application of various space technologies and often ground and airborne infrastructures broaden the space economy spectrum through value-added services sector.

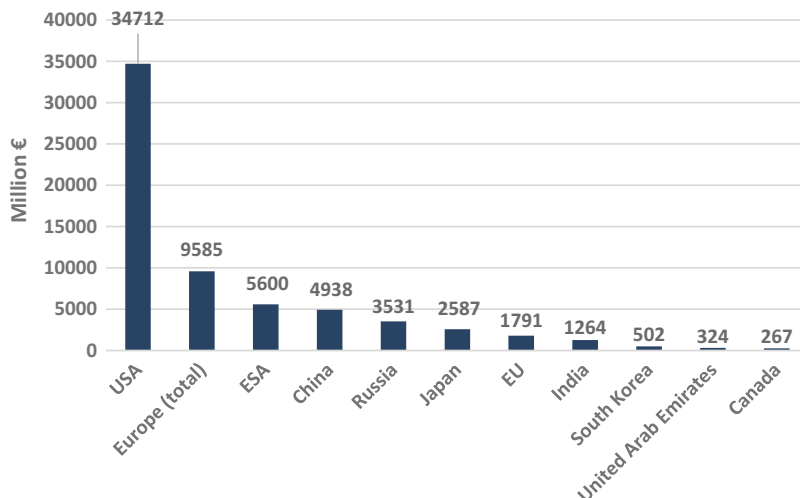
Worldwide national space budgets have continued to grow in 2017 and 2018. However, it is the commercial sector that is the primary cause for the overall growth of the space economy. The total figure for the global space economy in 2017 was \$383.51 billion (€339.48 billion) in government budgets and commercial revenue, an increase of 7.4% from the 2016 total of \$357.18 billion (€316.20 billion) and an increase of 31.6% compared to the 2013 figure of \$291.49 billion (€258.02 billion). (Exchange rate: \$1 = €1.1297, average for 2017 as provided by the European Central Bank. The average figure for the year(s) in question are used throughout the chapter when figures are converted between US\$ and Euros.) The majority of the increase in 2017 is attributable to growth in commercial sectors: commercial space products and services increased 8.3%, while commercial infrastructure and support industries increased by 7.5% (Space Foundation 2018). Overall, governmental spending increased from \$69.99 billion in 2017 to \$70.89 billion in 2018 (Euroconsult 2019). Overall, governmental spending, civilian and defense, increased by 4.8% from 2016 to 2017, although changes varied significantly from country to country, with India and China continuing their growth along with some ESA Member States. Many other space agencies, including those of the USA, Japan, Russia, and South Korea, saw a relative decrease from previous years signaling shifts in spending priorities. Such changes may be consequences of changing political climates affecting the economy and national institutional space activities. While the US figure decreased by 2.5% in 2017 compared to 2016, the total figure for non-US government space budgets increased by 16.4% (Space Foundation 2018, pp. 4–15) (Fig. 2).

## The Institutional Space Sector

Figure 3 shows government space expenditure in 2018, civil and defense (Euroconsult 2019). The ESA figure includes contributions from the EU. The countries spending the most on space in 2018 were the USA (€34.71 billion),



**Fig. 2** Global space activity 2017. (Source: Space Foundation 2018)



**Fig. 3** Public space budgets in 2019, civil and defense. (Source: Euroconsult 2019)

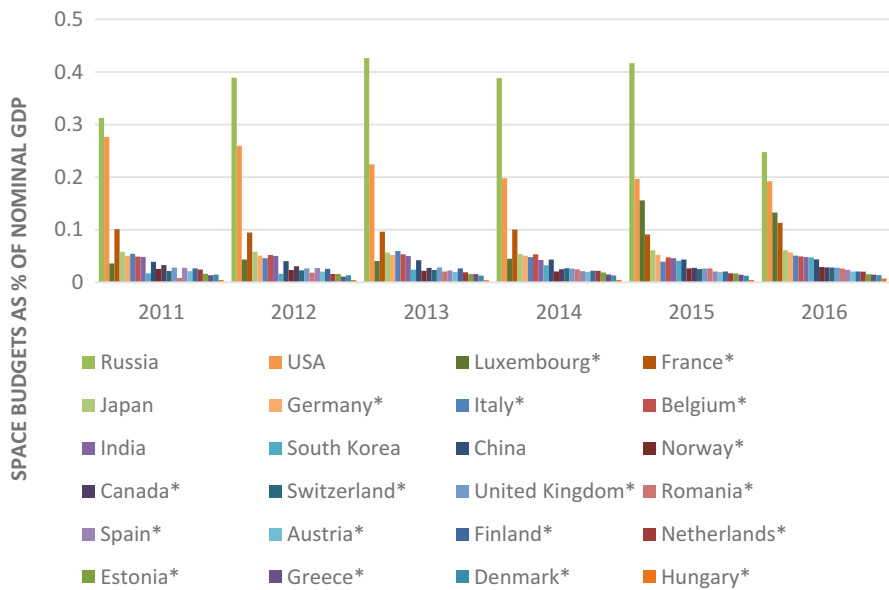
China (€4.94 billion), Russia (€3.53 billion), and Japan (€2.59 billion). The total figure for Europe mounted to €9.59 billion, while ESA's budget for the same year was €5.6 billion including contributions from the EU and others. This makes ESA the second largest civilian space agency in the world, following NASA. In 2017, according to the 2018 Space Report, the total world governmental expenditure, including that of intergovernmental organizations, on space programs amounted to \$76.20 billion (€53.9 billion), a figure which shows a nominal decrease of 1.78% compared to 2013. The space spending is comprised of \$48.54 billion (€42.97 billion) in civil expenditures, 64% of the total, and \$27.65 billion (€24.47 billion) in defense expenditures, 36% of the total, according to data gathered by the Space Foundation (2018). Of the estimated \$27.65 billion (€24.47 billion) of defense-related space expenditure worldwide, \$20.688 billion (€18.3 billion) was spent by the USA, most of it through the Department of Defence (DoD), representing a global share of 75%.

Data from 2019, gathered by Euroconsult, shows that the total figure for civilian government space expenditure mounted to \$44.49 billion (€37.67 billion) in 2018, up from \$42.63 billion (€36.07 billion) in 2017. In fact, civilian space budgets have increased since a low of \$39.14 billion (€35.28 billion) in 2015. Defense space budgets have also increased since 2015. In 2018, the total mounted to \$26.39 billion (€22.35 billion), which corresponds to about 37% of the total governmental spending for that year. This ratio varies significantly from the figures from the 2000s, where the ratio varies between 44.2% (2001) and 48.9% (2007). The last time this ratio was over 40% in 2012 (42.1%) (Euroconsult 2019). It should be noted, however, that these figures are based on accessible and public data and that differences in measurements and reporting are sources of potential errors when identifying and presenting global figures.

A prominent change in terms of the level of resources allocated to space is found in the growth of China's institutional space activities. The country's estimated total

doubled over 5 years from \$1.92 billion in 2008 to \$4.07 billion in 2013 and has continued to increase until 2018 (Euroconsult 2019). China is now the world’s second largest space country, following the USA, if one excludes the multilateral European activities undertaken by ESA. The USA has maintained its lead position with the largest budget among states, directing \$22.13 billion (€18.74 billion) towards civil expenditure and \$18.89 billion (€15.99 billion) towards defense expenditure. The low estimate of Russia’s budget must be put into perspective, as it does not factor in the intensive military activity entailing regular classified launches or the scientific programs. China’s national space budget reached €4.94 billion in 2018 and stays ahead of Russia (€3.53 billion) and Japan (€2.59 billion). The biggest governmental space expenditures in Europe are found in France (€2.67 billion), Germany (€1.82 billion), Italy (€0.95 billion), and the UK (€0.76 billion). The European Union has also become a major investor in space, with a total expenditure figure of €1.79 billion in 2018 (Euroconsult 2019). The 2019 budget for the European Space Agency (ESA), an intergovernmental organization with 22 Member States, mounts to €5.72 billion (ESA 2019). The largest contributors are France (€1.17 billion, 28.1%) and Germany (€0.93 billion, 22.2%), followed by Italy (€0.42 billion, 10.1%) and the UK (€0.37 billion, 8.8%). The total contribution from the EU, Eumetsat, and other nonstate actors is €1.53 billion (ESA 2019).

When measuring the concrete effort of countries in the space sector, it is necessary to put the figures into perspective in regard to Gross Domestic Product (GDP) (Fig. 4). However, considering the absolute numbers alone will paint only a partial



**Fig. 4** Government space budgets, civil and defense, as percentage of nominal GDP in 2018. (Sources: Euroconsult 2019; IMF 2018)

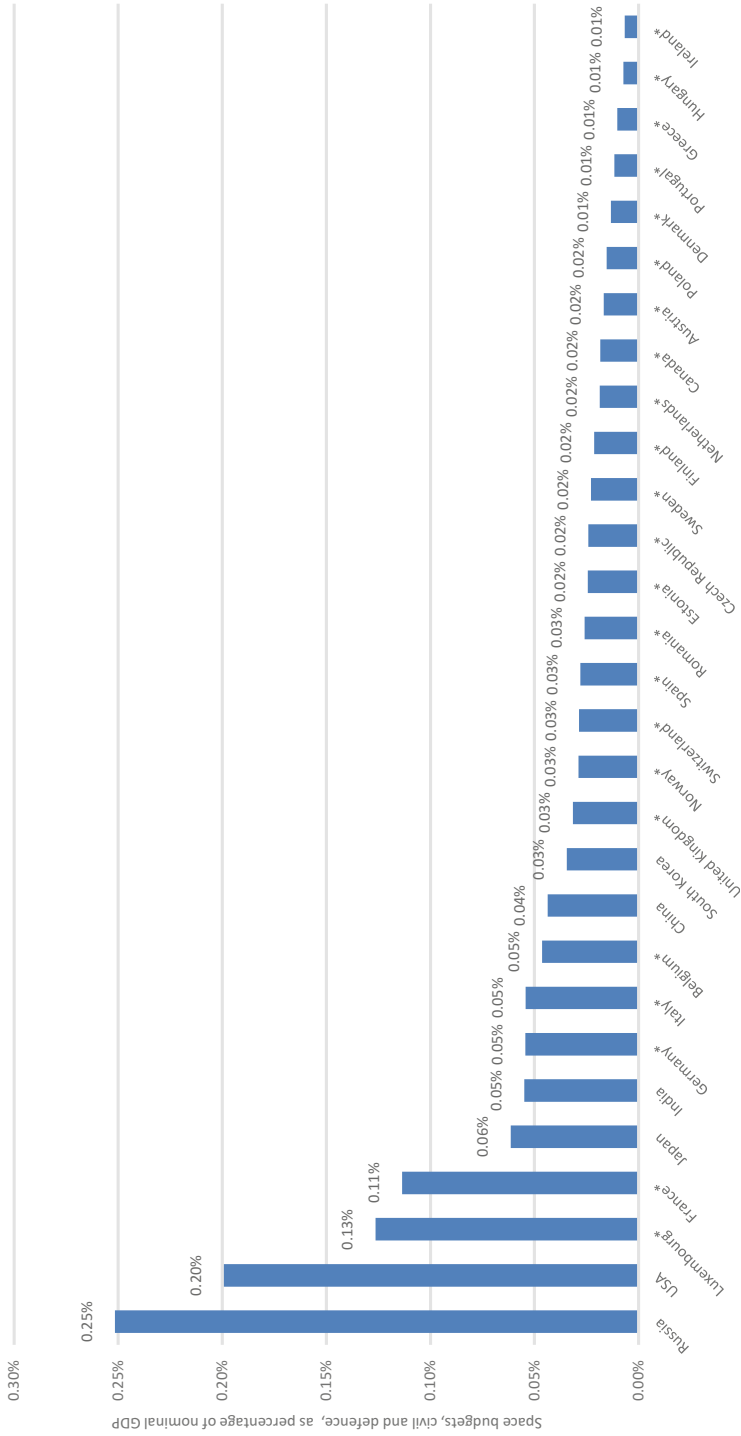
picture since comparisons between countries with different economic conditions (e.g., price or wage levels) can be misleading. National space budgets as share of GDP over time indicate how space is prioritized on the national level. As illustrated in Fig. 5, this ratio has remained relatively stable for most countries, with some exceptions. Two developments are standing out in Fig. 5. First, the Russian figure decreased significantly from 2015 to 2016, from 0.22% to 0.12%. Second, the figure for Luxembourg has increased significantly from 2013 onwards. In 2016, Luxembourg's civilian space budgets as a percentage of nominal GDP was third in rank after Russia and the USA. The remaining selected countries vary between 0.02% and 0.05%, with the exception of the French figure of 0.11%.

From the values listed in the Euroconsult report, combined with population data from the International Monetary Fund (IMF), the per capita budget of Luxembourg has been calculated to be €122.50. As illustrated in Fig. 6, Luxembourg and USA (€106.10) both spend significantly more on space relative to their respective populations compared to the other countries in this overview.

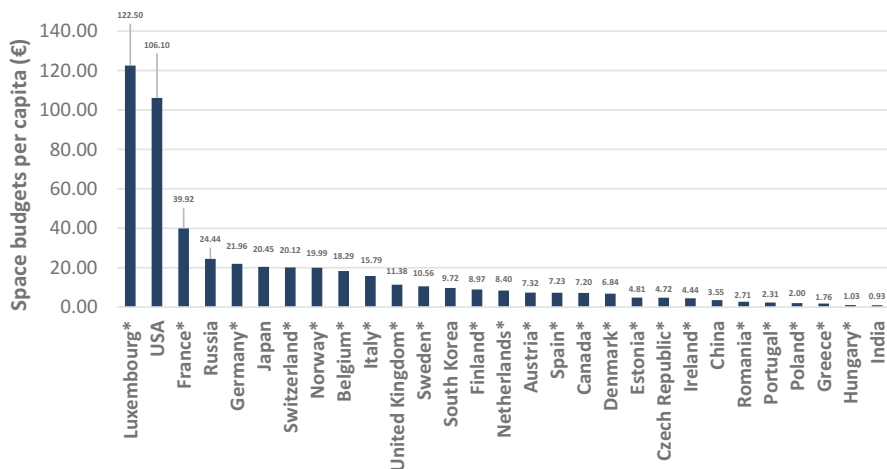
Space cannot be seen in isolation from research and development (R&D) policies. Figures 7, 8, and 9 show the civil space budget in relation to the government budget allocations for R&D (GBARD). Figure 7 shows the evolution of the civil space budgets as a percentage of civil GBARD for a number of selected countries. The evolution of civil space component of public R&D shows that civil space-related R&D budgets have picked in the early to mid-1990s then decreased. Since 2007 there is a decrease with the exception of the UK. According to the OECD (2018), the only three space powers where the civil space budget as a part of the GBARD outreaches the OECD average (7.95%) in 2016 are the USA, Italy (9.28), and Belgium (8.39%). (Data for Russia is not available.) Since 1981 as shown in Fig. 7, the USA has been in the lead, except for 2009 when the French figure was 14.9% and the US figure was 11.9%, both well above the OECD average of 7.1 at the time. The USA spends significantly less with regards to its civil GBARD in recent years compared to the 1990s, yet the figure has increased since the lowest point in 2009. In 2009, the figure for Japan was also higher than the OECD average. The financial crisis of 2009 could be one explanatory factor behind increased focus from governments on R&D, stimulating growth.

GBAORD data are assembled by national authorities and classified by “socio-economic” objectives on the basis of NABS 2007 (nomenclature for the analysis and comparison of scientific programs and budgets). The advantage of this is that they are reflecting government priorities.

Figure 9 shows space versus other areas of R&D expenditure according to Eurostat. This shows how space ranks as a priority within a country. The USA allocates most resources for R&D overall (€123.91 billion), followed by the combined figure for EU28 (€40.36 billion), Germany (€13.02 billion), Japan (€11.84 billion), United Kingdom (€8.50 billion), France (€6.62 billion), Italy (€5.09 billion), and Spain (€2.99 billion). For the exploration and exploitation of space, the USA spends €11.377 billion, followed by EU28 (€4.00 billion), Japan (€1.70 billion), Germany (€1.39 billion), and Italy (€929 million).



**Fig. 5** Space budgets, civil and defence, as percentage of nominal GDP for selected countries. ESA contributions are included for countries marked with “\*”. (Sources: World Bank 2019, Euroconsult 2017; IMF 2018)



**Fig. 6** Government space budgets, civil and defense, per capita in 2018. ESA contributions are included for countries marked with “\*”. (Sources: Euroconsult 2019; IMF 2018)

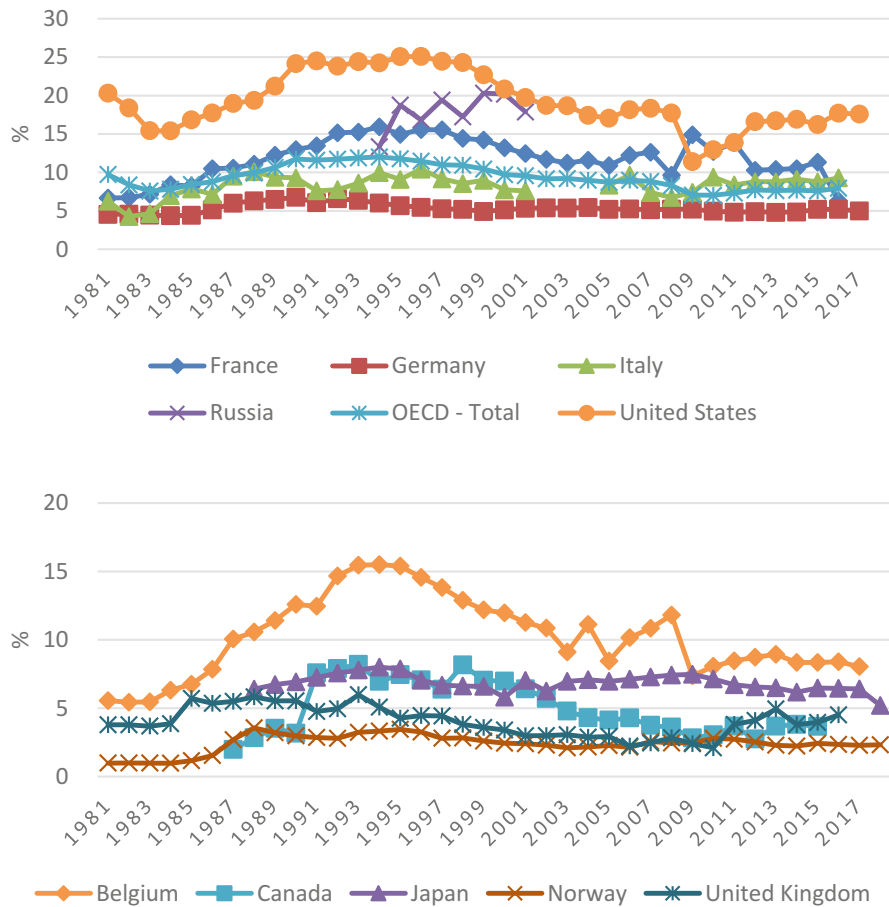
The main socioeconomic R&D objective in the EU is “industrial production and technology” (€9.69 billion), followed by “health” (€8.54 billion), “energy” (€4.66 billion), and “exploration and exploitation of space” (€4.00 billion) (Eurostat 2019).

Figure 10 shows government R&D priorities relative to each other within the same unit. Russian allocation for R&D funds suggest a very strong focus on space-related R&D relative to other objectives, while the trend in Europe is more general funds for universities and research institutions (OECD 2018).

The following tables (1, 2, and 3) give an overview of civil and defense government expenditures of recent years. Data is gathered from Euroconsult’s report Government Space Programs, Benchmarks, Profiles, and Forecasts to 2028, published in July 2019.

## The Commercial Space Sector

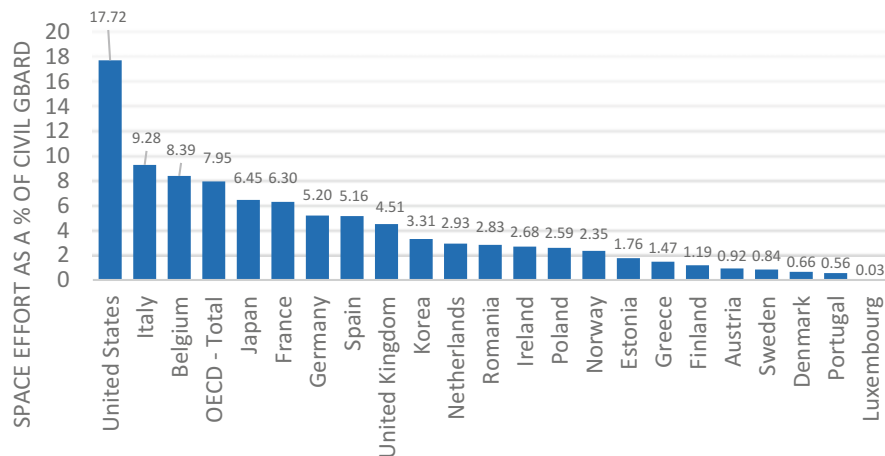
The space economy continues to grow as it has done for more than a decade, according to the Space Report 2018 published by the Space Foundation (p. 1). The greatest growth is found in the commercial space sector, where commercial space products and services make up 55.1% of the overall space activities in 2017. Combined with commercial infrastructure and support industries, the commercial sector accounts for 80% of total space activities amounting to \$307.32 billion (€272.04 billion). This is a 7,4% increase compared to the 2016 figure. For commercial space products and services, this represents a growth of 8.3% compared to 2016, while commercial infrastructure and support industries grew by 7.5% (ibid.). The Space Foundation (2018, p. 5) estimates the revenue of the global space activity in 2017 to \$383.51 billion (€339.48



**Fig. 7** Space as percentage of civil GBORD for selected countries, 1981–2017. (Source: OECD 2018)

billion), breaking the figure down in commercial space products and services (\$211.45 billion/€187.17 billion), commercial infrastructure and support industries (\$95.87 billion/€84.86 billion), US government space budgets (\$43.34 billion/€38.36 billion), and non-US government space budgets (\$32.85 billion/€29.08 billion).

For the commercial infrastructures and support industries, the highest proportion of revenues are generated in ground stations and equipment (\$85.84 billion/€75.98 billion) and satellite manufacturing (\$6.82 billion/€6.04 billion). The figure for the commercial satellite manufacturing represents 18.3% of the total value of the \$37.30 billion (€33.02 billion) spacecraft market in 2017, representing a significant growth of 41.2% from the 2016 figures of \$4.83 billion (€4.28 billion) (Space Foundation 2018). Commercial spacecraft is usually used for satellite communication, remote sensing or earth observation, commercial crew and cargo missions, launch vehicle



**Fig. 8** Space as percentage of civil GBARD for selected countries, 2016. (Source: OECD 2018)

test missions, or other purposes such as for countries without independent access to space (Federal Aviation Administration 2018).

The total figure for governmental space budgets in 2017 mounts to approximately \$76.2 billion (€67.45 billion). The USA is still in the lead with a total budget of about \$43.3 billion (€38.33 billion) of which about 47.8% is channelized through the Department of Defence (DoD) and about 45.3% through NASA. The three largest governmental or inter-governmental space agencies following the USA by share of the total global figure are China (10.5%), the European Space Agency (8.6%), and Japan (4.0%) (Space Foundation 2018).

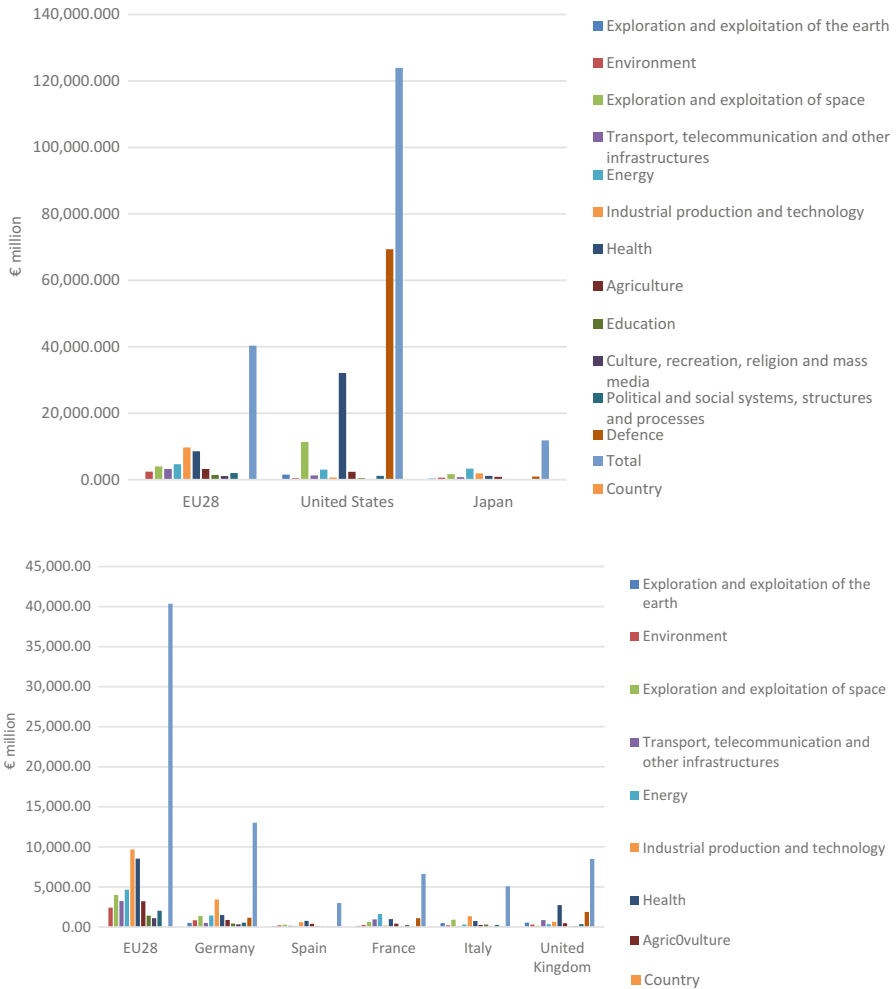
By country or territory of manufacturing, the USA and Europe are in the lead with 224 and 57 commercial spacecraft launched into orbit in 2017 (Space Foundation 2018). Combined, the USA and Europe represent 96% of the global manufacturing of commercial spacecraft, and the remaining 4% are manufactured in Argentina (1), China (6), Japan (3), and Russia (1). US launches represented 64% of commercial launches in 2017, while the European figure mounted to 24% (*ibid.*, p. 39). The USA is heading the hierarchy of launches with 29, followed by Russia (19), China (18), Europe (11), Japan (7), and India (5) (Figs. 11, 12, and 13).

Figure 11 presents the number of launches in 2017 by country and domain. There are no defense launches in Europe but there are payloads that can be considered under that category (for instance, OPTSAT-3000 VEGA launch for the Italian Defence Ministry).

According to the Union of Concerned Scientist (2019), there are 1,957 operational satellites in orbit per November 2018. The USA is in the lead with 849 satellites followed by Russia (152) and China (284). The number of payloads manufactured and launches by country in 2017 are illustrated in Fig. 12.

Figure 13 illustrates the number of noncommercial (civilian and defense) and commercial launches from 2012 to 2017. The number of commercial

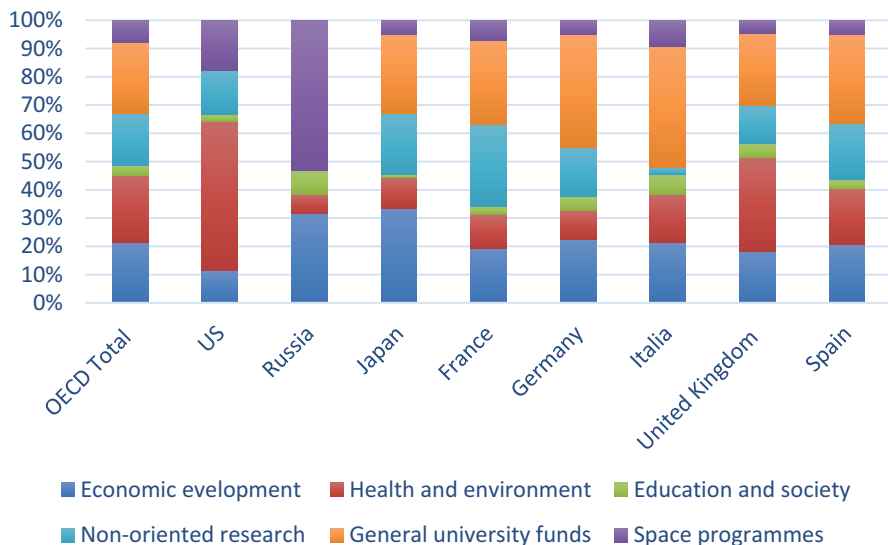




**Fig. 9** Space versus other areas of R&D expenditure, 2019. (Source: Eurostat 2019)

launches has been relatively stable between 2012 and 2016, before it increased significantly from 21 to 33 from 2016 to 2017, corresponding to an increase of 57%.

Although the annual number of launches has figured between 80 and 92 since 2012, the number of spacecraft launched into orbit has increased dramatically in 2017. A total of 469 spacecraft were launched in 2017, an increase by a factor of 2.54 compared to the 2016 figure. This growth is a consequence of a significant growth in commercial payloads launched in 2017 (Fig. 14). Moore’s law is also affecting the satellite industry (EIB Advisory 2018). This is reflected in the increase of small and very small (mini-, micro-, and nanoclass) payloads in clusters as 2017 was a record year for CubeSats, with 290 launched.



**Fig. 10** Space versus other domains of government R&D priorities, 2016. (Source: OECD 2018, p. 81)

## Forecasts for Government Space Budgets and Programs

The world total figure for government space budgets, civil and defense combined, continues to grow after some years of decline, posting 5 year CAGR of 5.75%. In the timeframe from 2008 to 2018, public budgets peaked in 2012 at \$68.95 billion (€53.67 billion), followed by years of declining budgets towards 2015 (\$62.50 billion/€56.33 billion). This decline towards 2015 can be explained by reduced defense space budgets in Russia and the USA. From 2016 onwards the total world figure has continued to increase and mounted \$70.89 billion (€60.03 billion) in 2018 (Euroconsult 2019). The ceiling point is likely to meet min 2020s (Fig. 15). (Euroconsult 2019)

When breaking down the total government expenditure figure by regions domain, in our case civil or defense budgets (although it can sometimes be difficult to code the budgets as either-or), we see broad trend lines as presented in Figs. 14, 15, 16, 17, and 18. As seen in the figures, the trend is increased spending in both civil and defense sectors. This trend, for the combined figure, is expected to last until the mid-2020s.

A few insights immediately strike they eye. First, the USA spends by far the most on defense space assets (Fig. 17) relative to any other countries in the world. However, the American share of global space budgets for defense has declined gradually from 83.8% in 2008 to 68.3 in 2018. Euroconsult (2019) predicts that this share will increase again in the years to come towards 2022. Second, the share of the total figure for civilian space budgets is far more distributed among the

**Table 1** Public space expenditure (civil + defense)

Countries	13	14	15	16	17	18
<b>NORTH AMERICA</b>	<b>35,782</b>	<b>35,839</b>	<b>35,594</b>	<b>37,198</b>	<b>38,152</b>	<b>41,311</b>
<b>Canada</b>	475	440	428	402	394	315
<b>United States</b>	35,307	35,399	35,165	36,796	37,759	40,996
<b>ASIA</b>	<b>8,899</b>	<b>9,284</b>	<b>9,967</b>	<b>10,593</b>	<b>11,013</b>	<b>11,771</b>
<b>Australia</b>	439	461	404	330	240	272
<b>Bangladesh</b>	25	29	63	63	67	70
<b>Cambodia</b>	0	0	0	0	0	4
<b>China</b>	4,069	4,574	4,860	5,145	5,450	5,833
<b>India</b>	916	870	964	1,092	1,295	1,493
<b>Indonesia</b>	54	75	70	73	79	205
<b>Japan</b>	2,907	2,585	2,824	3,005	3,047	3,056
<b>Korea</b>	317	485	553	643	589	593
<b>Laos</b>	0	0	17	17	17	17
<b>Malaysia</b>	10	10	10	10	10	10
<b>Mongolia</b>	23	50	50	53	55	5
<b>Myanmar</b>	0	0	0	0	0	0
<b>New Zealand</b>	4	4	4	7	9	9
<b>Pakistan</b>	11	11	26	38	33	61
<b>Philippines</b>	1	2	4	5	5	5
<b>Singapore</b>	22	34	33	18	16	29
<b>Taiwan</b>	59	51	39	31	35	35
<b>Thailand</b>	17	19	20	26	27	30
<b>Vietnam</b>	25	24	26	39	39	45
<b>CIS</b>	<b>10,189</b>	<b>7,357</b>	<b>5,000</b>	<b>4,278</b>	<b>4,768</b>	<b>4,355</b>
<b>Azerbaijan</b>	34	49	78	73	73	73
<b>Belarus</b>	21	21	22	23	23	28
<b>Kazakhstan</b>	284	214	22	45	47	50
<b>Russia</b>	9,753	6,966	4,790	4,122	4,609	4,170
<b>Turkmenistan</b>	67	88	74	5	5	5
<b>Ukraine</b>	31	18	14	10	10	28
<b>Uzbekistan</b>	0	0	0	0	0	2
<b>EUROPE</b>	<b>10,327</b>	<b>11,414</b>	<b>9,441</b>	<b>10,015</b>	<b>10,956</b>	<b>11,321</b>
<b>ESA</b>	4,580	4,415	3,583	4,205	4,238	4,465
<b>Eumetsat</b>	362	448	464	588	721	814
<b>Austria</b>	83	87	75	83	75	76
<b>Belgium</b>	279	282	216	231	248	247
<b>Bulgaria</b>	1	1	2	3	4	4
<b>Czech Republic</b>	24	25	21	23	59	59
<b>Denmark</b>	44	46	38	42	46	47
<b>Estonia</b>	4	5	4	3	6	7
<b>European Union</b>	1,584	2,729	2,160	1,929	2,100	2,115
<b>Finland</b>	72	60	48	49	55	58
<b>France</b>	2,975	3,072	2,391	2,782	3,055	3,158

(continued)

**Table 1** (continued)

Countries	13	14	15	16	17	18
<b>Germany</b>	1,988	2,000	1,816	1,963	2,127	2,151
<b>Greece</b>	42	41	35	20	24	22
<b>Hungary</b>	6	6	5	9	12	12
<b>Ireland</b>	28	28	24	30	25	25
<b>Italy</b>	1,274	1,032	719	945	1,116	1,127
<b>Lithuania</b>	4	4	5	6	7	5
<b>Luxembourg</b>	25	30	90	44	60	88
<b>Netherlands</b>	168	195	132	159	140	171
<b>Norway</b>	114	103	102	107	122	125
<b>Poland</b>	52	56	51	70	80	90
<b>Portugal</b>	27	28	23	23	26	28
<b>Romania</b>	31	42	39	41	48	62
<b>Slovakia</b>	3	3	3	5	5	6
<b>Slovenia</b>	5	4	4	4	9	13
<b>Spain</b>	309	303	257	321	337	399
<b>Sweden</b>	157	170	173	123	129	127
<b>Switzerland</b>	157	184	170	186	194	202
<b>UK</b>	871	877	839	814	844	894
<b>LATAM</b>	<b>706</b>	<b>793</b>	<b>1,058</b>	<b>744</b>	<b>562</b>	<b>426</b>
<b>Argentina</b>	243	240	254	142	148	110
<b>Bolivia</b>	34	25	50	37	47	44
<b>Brazil</b>	260	269	255	164	173	122
<b>Chile</b>	5	5	5	5	5	5
<b>Colombia</b>	2	2	2	2	3	3
<b>Ecuador</b>	8	7	7	7	7	7
<b>Mexico</b>	104	180	244	145	16	10
<b>Nicaragua</b>	0	0	0	0	26	83
<b>Paraguay</b>	0	2	2	2	2	2
<b>Peru</b>	4	18	55	74	61	7
<b>Venezuela</b>	47	45	186	166	75	33
<b>MIDDLE EAST AND AFRICA</b>	<b>1,277</b>	<b>1,221</b>	<b>1,437</b>	<b>1,533</b>	<b>1,549</b>	<b>1,699</b>
<b>Algeria</b>	47	58	83	74	67	75
<b>Angola</b>	34	34	46	36	35	42
<b>Bahrain</b>	0	1	1	1	1	2
<b>Egypt</b>	31	27	14	71	100	177
<b>Ethiopia</b>	1	2	2	1	2	3
<b>Gabon</b>	0	0	0	1	0	0
<b>Ghana</b>	1	1	1	2	2	2
<b>Iran</b>	220	193	138	132	118	142
<b>Israel</b>	212	154	168	159	77	77
<b>Kenya</b>	1	1	1	1	1	1
<b>Morocco</b>	58	97	133	136	143	80
<b>Nigeria</b>	73	69	48	53	42	48

(continued)

**Table 1** (continued)

Countries	13	14	15	16	17	18
<b>Oman</b>	0	0	0	0	0	1
<b>Qatar</b>	75	33	117	179	200	186
<b>Saudi Arabia</b>	15	15	51	130	166	165
<b>South Africa</b>	22	35	35	31	36	36
<b>Tunisia</b>	1	1	1	1	1	2
<b>Turkey</b>	380	350	253	136	148	276
<b>UAE</b>	106	151	347	389	409	383
<b>Zimbabwe</b>	0	0	0	0	0	1
<b>TOTAL</b>	<b>67,181</b>	<b>65,907</b>	<b>62,497</b>	<b>64,361</b>	<b>67,000</b>	<b>70,883</b>

Source: Euroconsult 2019

continents, although North America is still in lead in 2018 with 50.3%, followed by Europe (22.5%), Asia (18.6%), the CIS countries (Azerbaijan, Belarus, Kazakhstan, Russia, Turkmenistan, Ukraine, and Uzbekistan) (5.4%), the Middle East and Africa (2.4%), and Latin America (0.8%). Third, the space budgets for both civilian and defense purposes tends to follow the same paths; overall growth and overall decline across the board. As seen in the figures, Euroconsult (2019) foresees that government spending will continue to increase towards the mid-2020s, from the low of \$62.50 billion (€56.33 billion) in 2015 to \$84.59 in 2025. The decline from 2025 onwards is due to expected decreases in defense space spending, while the civilian budgets are expected to continue to grow towards 2030.

Euroconsult (2019, p. 8) predicts that the civil space budgets, overall, will grow at an average of 1.6% every year towards 2030, while defense space budgets will grow at an average yearly rate of 4.2% towards the mid-2020s followed by a negative growth. Investments in space science, exploration, and human spaceflight are drivers behind the civilian growth. The steady growth in defense budgets is predicted based on defense budget cycles in Asian, the Middle East, and the USA. The total 10-year CAGR 2019–2028 is expected to be 2.39%, civil and defense combined, in contrast to the high 11.8 CAGR of the 1999–2008 period (Euroconsult 2019, p. 12). (Compound annual growth rate (CAGR) is the average year-over-year rate of the investment over a specified period of time.)

The USA remains the largest investor in space activities, followed by China, Russia, France, and Japan. In 2018, the number of satellites (over 50 kg) launched mounted to 138, an 84% increase compared to the 75 satellites launched in 2017 (Euroconsult 2019). In the course of 2018 and 2019, Greece, Luxembourg, Australia, Zimbabwe, Turkey, and Portugal have established national space agencies.

In the area of defense space programs, funding is expected to increase until 2025. Already from 2017 to 2018, the world total for space defense budgets increased by 8.3%. The USA is dominating with 71.7% of the world total, and space defense activities are supported by the Trump administration (Euroconsult 2019, p. 15). In relative terms, Asian spending on military space activities has more than doubled over the period between 2008 and 2018, strongly driven by China along with

**Table 2** Civil space expenditure

Countries	13	14	15	16	17	18
<b>NORTH AMERICA</b>	<b>18,609</b>	<b>19,494</b>	<b>19,716</b>	<b>21,068</b>	<b>21,380</b>	<b>22,398</b>
<b>Canada</b>	388	330	322	294	272	269
<b>USA</b>	18,222	19,163	19,394	20,774	21,108	22,129
<b>ASIA</b>	<b>6,034</b>	<b>6,443</b>	<b>6,838</b>	<b>7,397</b>	<b>7,722</b>	<b>8,278</b>
<b>Australia</b>	304	430	377	240	97	116
<b>Bangladesh</b>	25	29	63	63	67	70
<b>Cambodia</b>	0	0	0	0	0	4
<b>China</b>	2,392	2,665	2,788	2,994	3,441	3,699
<b>India</b>	829	811	904	1,030	1,227	1,406
<b>Indonesia</b>	53	74	69	72	65	177
<b>Japan</b>	1,947	1,749	1,859	2,117	1,994	2,017
<b>Korea</b>	317	485	553	643	589	551
<b>Laos</b>	0	0	17	17	17	17
<b>Malaysia</b>	10	10	10	10	10	10
<b>Mongolia</b>	23	50	50	53	55	5
<b>New Zealand</b>	0	0	0	2	5	5
<b>Pakistan</b>	11	11	26	38	33	61
<b>Philippines</b>	1	2	4	5	5	5
<b>Singapore</b>	22	34	33	18	16	26
<b>Taiwan</b>	59	51	39	31	35	35
<b>Thailand</b>	17	19	20	26	27	30
<b>Vietnam</b>	25	24	26	39	39	45
<b>CIS</b>	<b>5,626</b>	<b>3,778</b>	<b>2,343</b>	<b>2,095</b>	<b>2,524</b>	<b>2,391</b>
<b>Azerbaijan</b>	34	49	78	73	73	73
<b>Belarus</b>	21	21	22	23	23	28
<b>Kazakhstan</b>	284	214	22	45	47	50
<b>Russia</b>	5,189	3,387	2,133	1,939	2,365	2,206
<b>Turkmenistan</b>	67	88	74	5	5	5
<b>Ukraine</b>	31	18	14	10	10	28
<b>Uzbekistan</b>	0	0	0	0	0	2
<b>EUROPE</b>	<b>9,108</b>	<b>9,920</b>	<b>8,445</b>	<b>8,855</b>	<b>9,587</b>	<b>10,014</b>
<b>ESA</b>	4,580	4,415	3,583	4,205	4,238	4,465
<b>Eumetsat</b>	362	448	464	588	721	814
<b>Austria</b>	83	87	75	83	75	76
<b>Belgium</b>	279	282	216	231	248	247
<b>Bulgaria</b>	1	1	2	3	4	4
<b>Czech Republic</b>	24	25	21	23	59	59
<b>Denmark</b>	42	45	37	41	45	46
<b>Estonia</b>	4	5	4	3	6	7
<b>European Union</b>	1,584	2,729	2,160	1,929	2,100	2,115
<b>Finland</b>	72	60	48	49	55	58
<b>France</b>	2,432	2,346	2,047	2,251	2,373	2,517
<b>Germany</b>	1,897	1,898	1,695	1,799	1,873	1,964

(continued)

**Table 2** (continued)

Countries	13	14	15	16	17	18
<b>Greece</b>	27	25	19	20	24	22
<b>Hungary</b>	6	6	5	9	12	12
<b>Ireland</b>	28	28	24	30	25	25
<b>Italy</b>	1,082	786	629	848	1,042	1,071
<b>Lithuania</b>	4	4	5	6	7	5
<b>Luxembourg</b>	23	27	33	28	44	56
<b>Netherlands</b>	165	192	129	157	138	169
<b>Norway</b>	100	90	92	98	113	116
<b>Poland</b>	52	56	51	70	80	90
<b>Portugal</b>	27	28	23	23	26	28
<b>Romania</b>	31	42	39	41	48	62
<b>Slovakia</b>	3	3	3	5	5	6
<b>Slovenia</b>	5	4	4	4	9	13
<b>Spain</b>	269	254	213	256	271	331
<b>Sweden</b>	157	170	173	123	129	127
<b>Switzerland</b>	157	184	170	186	194	202
<b>UK</b>	553	542	528	539	582	585
<b>LATAM</b>	<b>691</b>	<b>738</b>	<b>933</b>	<b>584</b>	<b>421</b>	<b>337</b>
<b>Argentina</b>	243	240	254	142	148	110
<b>Bolivia</b>	34	25	50	37	47	44
<b>Brazil</b>	260	244	196	89	104	52
<b>Colombia</b>	2	2	2	2	3	3
<b>Ecuador</b>	2	1	1	1	1	1
<b>Mexico</b>	104	180	244	145	16	10
<b>Nicaragua</b>	0	0	0	0	26	83
<b>Paraguay</b>	0	2	2	2	2	2
<b>Venezuela</b>	47	45	186	166	75	33
<b>MIDDLE EAST AND AFRICA</b>	<b>817</b>	<b>820</b>	<b>866</b>	<b>929</b>	<b>998</b>	<b>1,074</b>
<b>Algeria</b>	47	58	83	74	67	75
<b>Angola</b>	34	34	46	36	35	42
<b>Bahrain</b>	0	1	1	1	1	2
<b>Egypt</b>	31	27	14	23	46	57
<b>Ethiopia</b>	1	2	2	1	2	3
<b>Gabon</b>	0	0	0	1	0	0
<b>Ghana</b>	1	1	1	2	2	2
<b>Iran</b>	220	193	138	132	118	142
<b>Israel</b>	18	24	35	40	39	38
<b>Morocco</b>	3	3	3	3	3	3
<b>Nigeria</b>	73	69	47	52	37	41
<b>Oman</b>	0	0	0	0	0	1
<b>Qatar</b>	75	33	54	100	121	107
<b>Saudi Arabia</b>	15	15	51	130	166	165
<b>South Africa</b>	22	35	35	31	36	36

(continued)

**Table 2** (continued)

Countries	13	14	15	16	17	18
<b>Tunisia</b>	1	1	1	1	1	2
<b>Turkey</b>	248	261	200	103	115	183
<b>UAE</b>	27	62	156	198	209	174
<b>Zimbabwe</b>	0	0	0	0	0	1
<b>TOTAL</b>	40,884	41,191	39,140	40,928	42,632	44,492

Source: Euroconsult 2019

significant Japanese budget allocations, and is expected to increase further from \$3.49 billion to \$5.19 billion in 2025. Europe is the fourth largest region in terms of space defense spending, totaling \$1.30 billion following the USA, Asia, and CIS countries (Russia). Ariane 6 development is approaching its final phase, which may lead to reduced defense space contributions in Europe. The foreseen growth in space defense spending is mainly driven by the USA, China, India, and Japan (Euroconsult 2019, p. 15).

In terms of domains of the various programs, for launch vehicles, the total funding in 2018 corresponded to \$6.71 billion (€5.68 billion), split between civil (60%), and defense (40%) domains. Euroconsult (2019) expects this figure to peak in 2019 at \$7.04 billion due to the completion of the European Ariane 6 launcher foreseen in 2020, dropping to \$6.02 billion in 2020.

With a 2018 total funding of \$11.77 billion (€9.97 billion), Earth Observation (including metrological missions) programs remains the highest funded space application overall (Euroconsult 2019, p. 18). The figure will decrease on the short term, due to reduced funding over the US budget, yet this effect will, to a certain degree, be counterweighted by increased spending in Europe, Asia, and the Middle East and Africa. Defense spending is expected to experience a significant boost from \$2.78 billion in 2021 to \$3.54 in 2022.

For satellite communication, Euroconsult (2019, p. 19) anticipates an overall growth from \$5.82 billion (€4.92) in 2018 to \$8.29 billion in 2025. The defense figures for satellite communication make 63.3% of the total world spending in 2018. The total figure has declined from 2011 (\$9.36 billion/€6.72 billion), and this is mainly due to procurement cycles of the US Department of Defence. In 2011, the defense spending corresponded to 75.6% of the overall spending. The ratio between civil and defense expenditure is expected to remain rather stable, and the growth is foreseen with the basis of more and more countries investing in satcom capabilities.

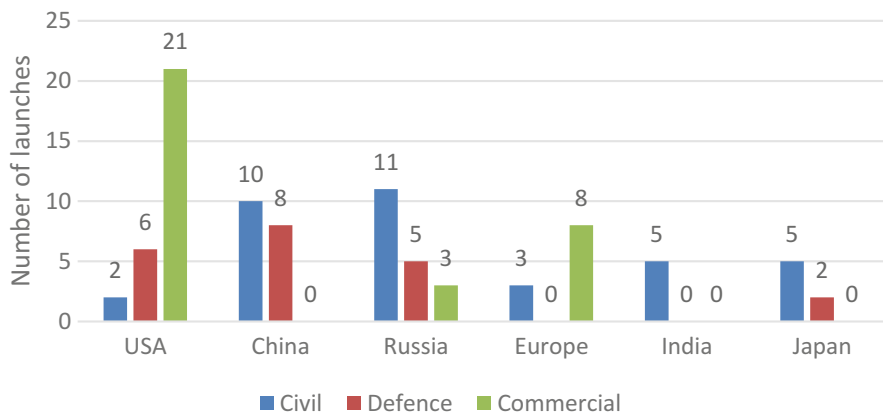
In the area of satellite navigation, funding has declined since the peak year or 2014 and the total figure of \$4.67 billion (€3.52 billion). This year, the EU accounted for almost half the expenditures (45%), funding that was spent on its Galileo flagship program. Galileo is foreseen to be fully operational in the early 2020s. A GNSS constellation requires extensive funding associated with development, launches, and operations, which limits the number of countries willing to pursue such capabilities. The 2018 GNSS spending figure for civilian and defense programs was \$3.63 billion



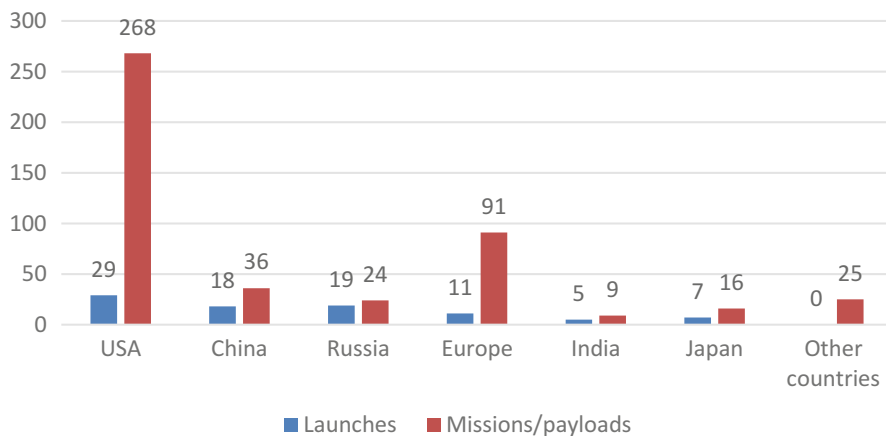
**Table 3** Defence space expenditure

Countries	13	14	15	16	17	18
<b>NORTH AMERICA</b>	<b>17,173</b>	<b>16,345</b>	<b>15,878</b>	<b>16,130</b>	<b>16,773</b>	<b>18,913</b>
Canada	87	109	106	108	122	46
USA	17,086	16,236	15,772	16,022	16,651	18,867
<b>ASIA</b>	<b>2,866</b>	<b>2,841</b>	<b>3,129</b>	<b>3,196</b>	<b>3,291</b>	<b>3,493</b>
Australia	135	31	28	90	143	156
China	1,677	1,909	2,071	2,151	2,009	2,134
India	87	60	60	62	68	87
Indonesia	1	1	1	1	14	28
Japan	961	836	965	888	1,053	1,039
Korea	0	0	0	0	0	42
New Zealand	4	4	4	4	4	4
Singapore	0	0	0	0	0	3
<b>CIS</b>	<b>4,564</b>	<b>3,579</b>	<b>2,657</b>	<b>2,183</b>	<b>2,244</b>	<b>1,964</b>
Russia	4,564	3,579	2,657	2,183	2,244	1,964
<b>EUROPE</b>	<b>1,219</b>	<b>1,494</b>	<b>996</b>	<b>1,160</b>	<b>1,368</b>	<b>1,307</b>
ESA	0	0	0	0	0	0
Eumetsat	0	0	0	0	0	0
Denmark	1	1	1	1	1	1
European Union	0	0	0	0	0	0
France	543	726	344	531	682	641
Germany	92	102	121	164	255	188
Greece	15	16	16	0	0	0
Italy	191	247	90	96	74	56
Luxembourg	3	3	58	16	16	32
Netherlands	2	2	2	2	2	2
Norway	14	13	10	10	10	10
Spain	40	49	44	65	66	69
UK	318	335	311	275	262	308
<b>LATIN AMERICA</b>	<b>15</b>	<b>55</b>	<b>125</b>	<b>161</b>	<b>141</b>	<b>89</b>
Brazil	0	26	59	75	69	70
Chile	5	5	5	5	5	5
Ecuador	6	6	6	6	6	6
Peru	4	18	55	74	61	7
<b>MIDDLE EAST AND AFRICA</b>	<b>461</b>	<b>402</b>	<b>571</b>	<b>604</b>	<b>551</b>	<b>626</b>
Egypt	0	0	0	48	54	120
Israel	194	129	133	118	39	39
Kenya	1	1	1	1	1	1
Morocco	55	94	130	133	140	77
Nigeria	0	0	1	1	5	7
Qatar	0	0	63	79	79	79
Turkey	132	89	53	33	33	93
UAE	79	89	191	191	200	210
<b>TOTAL</b>	<b>26,297</b>	<b>24,716</b>	<b>23,357</b>	<b>23,434</b>	<b>24,368</b>	<b>26,391</b>

Source: Euroconsult 2019



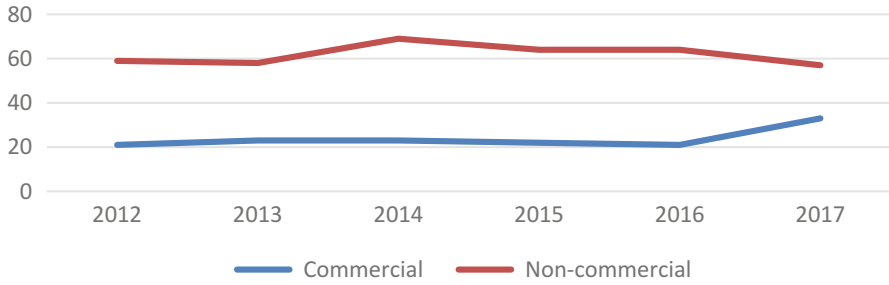
**Fig. 11** Launches in 2017 by country and domain. (Source: Federal Aviation Administration 2018)



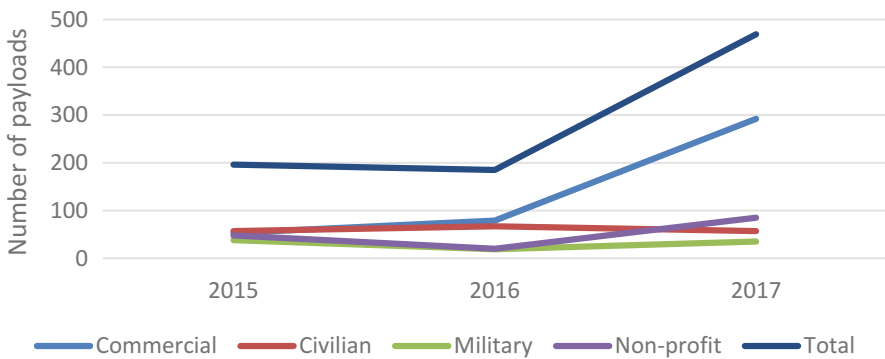
**Fig. 12** Launches and payloads in 2017 (“other” countries refers to Argentina, Australia, Canada, Chile, Ecuador, Israel, Kazakhstan, South Africa, South Korea, Taiwan, Turkey, UAE, and Ukraine). (Source: Federal Aviation Administration 2018)

(€3.07 billion), and this figure is expected to grow towards, and peak at, \$4.69 in 2026 (Euroconsult 2019, p. 19).

Science and exploration are funded over civilian budgets. The global expenditure mounted \$7.0 billion (€5.93 billion) in 2018 and is overall expected to grow towards 2028 (expected \$8.66 billion). Although about 28 countries invest in space science and exploration, the major six players account for almost all the spending (about 95%). This is, according to Euroconsult (2019, p. 18), due to the fact that these missions are highly visible thus suitable for public communication campaigns, while at the same time being ambitious.



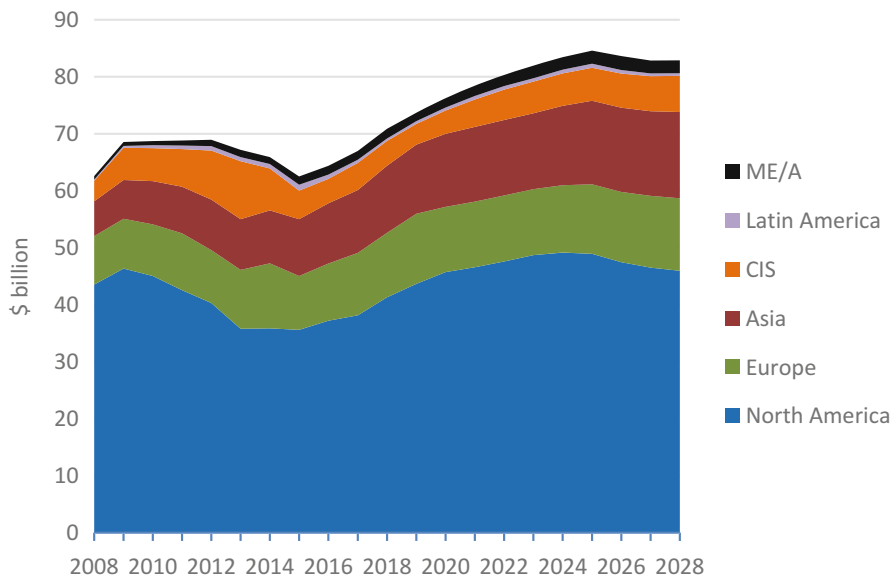
**Fig. 13** Commercial and noncommercial launches 2012–2017. (Sources: Federal Aviation Administration 2012, 2013, 2014, 2016, 2017, 2018)



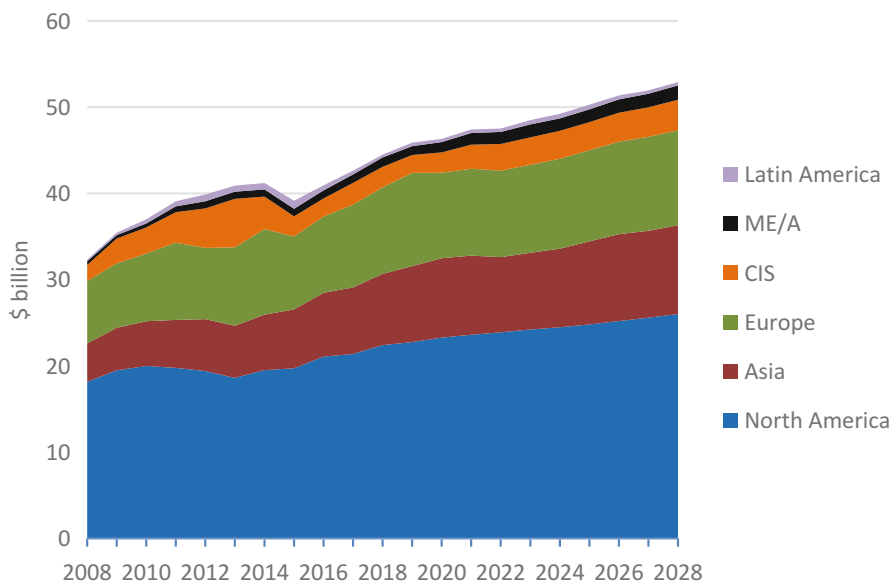
**Fig. 14** Spacecraft launched 2015–2017. (Sources: Federal Aviation Administration 2016, 2017, 2018)

Human space flight is, after Earth Observation, the second single largest domain for space expenditures, totaling \$11.56 billion (€9.79 billion) in 2018. The US proportion is about 77%, slightly down from 80% 2 years before, in part due to new actors entering the field including the United Arab Emirates. A significant and stable increase in spending is foreseen for the coming 10 years, mainly because of the manifestation of post-ISS activities such as the Lunar Gateway in the coming years. In 2028, Euroconsult (2019, p. 18) foresee the expenditure figures to reach \$16.96 billion.

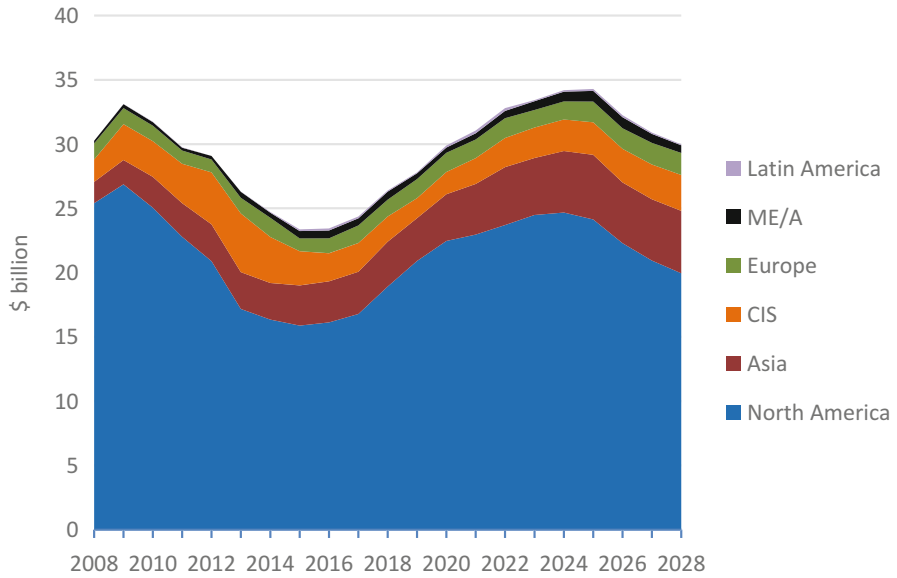
Space security, including early warning, is one of the most geographically concentrated domains in terms of expenditure, dominated by the USA, Russia, and France. As more countries express interest in space and security, and budgets increase in Asia, Europe, and Russia, the US dominance in the domain is likely to decline towards 2028. European countries, through the multilateral frameworks of ESA and the EU, have, for instance, demonstrated very keen interest in space security initiatives (including SSA for the EU) (Euroconsult 2019, p. 19). Budgets are expected to grow from \$2.10 billion (€1.78 billion) in 2018, to \$4.24 billion in 2023, before a decline towards the expected figure of \$2.51 in 2028 (Table 4).



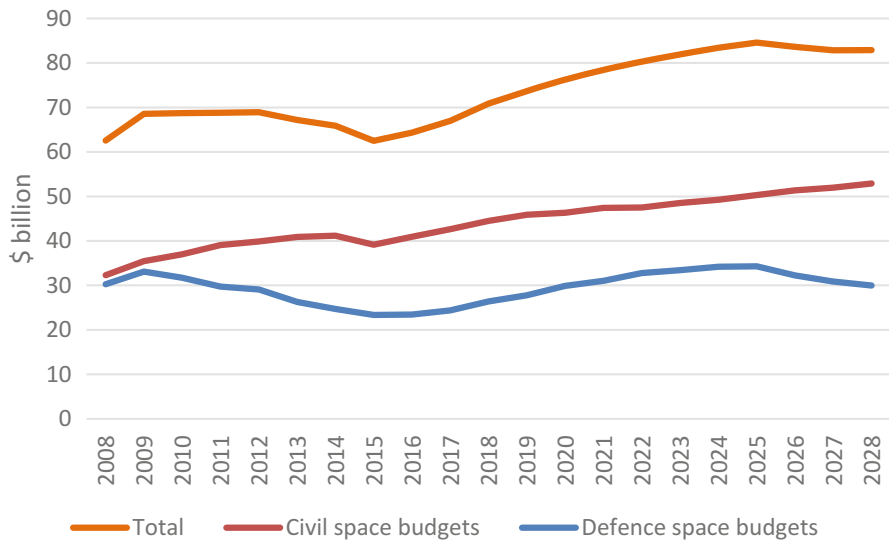
**Fig. 15** Historical and forecast for government space expenditures by region, civil and defense, 2008–2028. (Source: Euroconsult 2019)



**Fig. 16** Historical and forecast for civil government space expenditures by region, 2008–2028. (Source: Euroconsult 2019)



**Fig. 17** Historical and forecast for defense government space expenditures by region, 2008–2028. (Source: Euroconsult 2019)



**Fig. 18** Historical and forecast for civil and defense government space expenditure, 2008–2028. (Source: Euroconsult 2019)

**Table 4** Exchange rates for relevant years

Year	Exchange rate (1€ = X.XXXX\$)	1\$ = X.XXXX€
2011	1.3920	0.718
2012	1.2848	0.778
2013	1.3281	0.753
2014	1.3285	0.753
2015	1.1095	0.901
2016	1.1069	0.903
2017	1.1297	0.885
2018	1.1810	0.8467
2019	1.1224	0.891

Source: European Central Bank

## Conclusions

Accurate estimate of global space activities is a complicated task. This is due to the fact that there is lack of a standardized approach and lack of transparency in certain government space programs, such as defense-related programs. Additionally, the publication of financial figures by commercial companies is not uniform across the sector and varies in time. However, two trends stand out when investigating the space economy. First, government space budgets peaked in 2012, followed by decline, and is now increasing again and forecasts suggest that it will continue to grow in the years to come. Second, the commercial space sector constitutes the largest share of the economy with the emergence of new actors and more private investments. 2017 experienced a significant increase of commercial spacecraft launched to orbit. There also seems to be a growing interest on the recent private investments with companies such as SpaceX and Blue Origin as new drivers for the pace of the space economy. However, this must be put into perspective. While they are significant investment as compared to other private companies in the world, they still largely depend on government funding (80% for SpaceX) and do not reach government level (Fiorasco 2016). Although private space sector continues to grow, governments remain crucial actors in the space field.

## References

- Euroconsult (2017) Government space programs: benchmarks, profiles & forecasts to 2026. Euroconsult, Paris
- Euroconsult (2019) Government space programs: benchmarks, profiles & forecasts to 2028. Euroconsult, Paris
- European Commission (2018) EU budget: a €16 billion Space Programme to boost EU space leadership beyond 2020, Brussels. [http://europa.eu/rapid/press-release\\_IP-18-4022\\_en.htm](http://europa.eu/rapid/press-release_IP-18-4022_en.htm). Accessed 4 Mar 2019

- European Investment Bank Advisory Group (2018) *The Future of the European Space Sector: How to leverage Europe's Technological leadership and boost investments for space ventures*. EIB, Luxembourg
- European Space Agency (2017) *ESA long-term plan 2018–2027*. ESA, Paris. ESA/C(2017)96
- European Space Agency (2019) *ESA budget for 2019*. [http://www.esa.int/ESA\\_Multimedia/Images/2019/01/ESA\\_Budget\\_2019](http://www.esa.int/ESA_Multimedia/Images/2019/01/ESA_Budget_2019). Accessed 24 Oct 2019
- Eurostat (2019) *R&D expenditure*. [https://ec.europa.eu/eurostat/statistics-explained/index.php/R\\_%26\\_D\\_expenditure](https://ec.europa.eu/eurostat/statistics-explained/index.php/R_%26_D_expenditure). Accessed 20 Oct 2019
- Federal Aviation Administration (2012) *The annual compendium of commercial space transportation: 2012*. Federal Aviation Administration, Washington, DC
- Federal Aviation Administration (2013) *The annual compendium of commercial space transportation: 2012*. Federal Aviation Administration, Washington, DC
- Federal Aviation Administration (2014) *The annual compendium of commercial space transportation: 2013*. Federal Aviation Administration, Washington, DC
- Federal Aviation Administration (2016) *The annual compendium of commercial space transportation: 2016*. Federal Aviation Administration, Washington, DC
- Federal Aviation Administration (2017) *The annual compendium of commercial space transportation: 2017*. Federal Aviation Administration, Washington, DC
- Federal Aviation Administration (2018) *The annual compendium of commercial space transportation: 2018*. Federal Aviation Administration, Washington, DC
- Fiorasco G (2016) *Open space, L'ouverture comme reponse aux defies de la filiere spatiale*. Rapport au Premier ministre, Paris
- Hatzichronoglou T (1997) *Revision of the high technology sector and product classification*. OECD Publishing, Paris
- IMF (2018) *World economic outlook*. Washington, DC. <https://www.imf.org/external/pubs/ft/weo/2018/02/weodata/index.aspx>. Accessed 4 Mar 2019
- Organisation for Economic Co-operation and Development (2011) *Main science and technology indicators database*. <http://www.oecd.org/sti/msti.htm>. Accessed 4 Mar 2019
- Organisation for Economic Co-operation and Development (2016) *Space and innovation*. OECD, Paris
- Organisation for Economic Co-operation and Development (2018) *Main Science and Technology Indicators*. Volume 2018/1. OECD, Paris
- Space Foundation (2016) *The space report: the authoritative guide to global space activity*. The Space Foundation, Colorado Springs
- Space Foundation (2018) *The space report: the authoritative guide to global space activity*. The Space Foundation, Colorado Springs
- Union of Concerned Scientists (2019) *UCS satellite database*. <https://www.ucsusa.org/nuclear-weapons/space-weapons/satellite-database#.XFHCsL4vw2w>. Accessed 4 Mar 2019
- World Bank (2019) *Population estimates and projections database*. <https://datacatalog.worldbank.org/dataset/population-estimates-and-projections>. Accessed 4 July 2019



# The New Space Economy: Consequences for Space Security in Europe

# 74

Jean-Pierre Darnis

## Contents

Introduction .....	1500
The New Space Economy: A Push Coming from the USA .....	1500
The Transformation of Space Security .....	1502
European Space: A Resilient Model .....	1504
Conclusion .....	1508
References .....	1510

## Abstract

The “new space economy” as a new paradigm able to revolutionize space activities shall be discussed. There is a large consensus of perceptions which tends to define this set of US-led policies and investments as a shift for all space activities. This is the reason why it triggers effects worldwide and creates a new context for European space activities. In Europe, space policies have often been characterized by a dialectic between plurality and collaborative common frameworks. Large European Union member countries such as France, Germany, and Italy have developed a space policy on a national basis, although they traditionally collaborate through ESA, an international intergovernmental organization. More recently, the European Union, which does not share the same membership and rules as ESA, has stepped into space activities. These three layers help us define a fragmented European space panorama, which has always found it difficult to respond to the critical mass developed by US public and private policies. This is today the case with the “new space economy,” where the USA is fundamentally renewing its public policy in order to create a more efficient and business-friendly approach to space, a shift which has helped create a new breed of space entrepreneurs, IT

J.-P. Darnis (✉)

Université Côte d’Azur, Istituto Affari Internazionali (IAI), Nice, France

e-mail: [darnis@unice.fr](mailto:darnis@unice.fr)



tycoons investing in space with considerable financial capabilities, and tech incubator methodologies. This paradigm has renewed investments, technologies, and a new spirit of space conquest and puts enormous pressure on the European space sector, which has to renew its classic approach. Europe needs to come up with a more strategic space vision that is able to take into account not only the outcomes of new technology but also the inbred characteristics of space-based technology production and data fluxes, with key issues in terms of security.

---

## Introduction

The “new space economy” represents a flashy and highly mediatized phenomenon. The image of the Starman piloting a Tesla roadster in space after being launched by Elon Musk Falcon Heavy rocket looks like a glimpse of a future able to create worldwide empathy among space geeks and public opinion. Behind this glamorous image, the “new space economy” describes an interesting phenomenon, which comes from a public policy reform of space and the increase of technological companies and investors in the USA. Building upon a massive capacity for public investment (space budgets, civilian, and military are roughly between 40 and 50 billion dollars a year), the USA is pushing the policy even further when Donald Trump speaks of “American dominance in space.” On the European side, space has always been developed through a softer, if not blander, approach characterized by three pillars: an important European Space Agency (ESA) which has framed scientific exploration and technological research in space; some key member states such as France, Germany, and Italy which developed similar but autonomous space policies, also in the defense realm; and an emerging role from the European Commission which has fostered a “service to citizens” approach in its development of two flagship programs like Galileo and Copernicus. While for Europe security could appear as one of the services offered by space-based products, the US paradigm shift brings up not only a potential acceleration in terms of financial and technological fluxes but also the development of a more global “space security” considering the infrastructure, the data, and the products as a whole.

While European space policy can be seen as a very positive phenomenon, both in terms of outcomes and also for the political cooperative effort which has always characterized space, the post “new space economy” model illustrates the need to further intensify the cooperation framework, the goal being to develop a European way to a “global space strategy” without being pulled aside by the harvesting of data potentially coming from the USA and China.

---

## The New Space Economy: A Push Coming from the USA

The “new space economy” is often presented as a new paradigm for space policy (Pasco 2017). It is a remarkable example of a public policy shift, which started in 2004 when the USA decided to put an end to space shuttle activities and

progressively reoriented its access to space activities (Sehovic 2018). NASA became a customer buying launching capabilities from private companies rather than developing its own vehicles. Since then, the Commercial Orbital Transportation Services (COTS) program, followed by the Commercial Crew Development (CCDeV) program, has developed and shaped new bidding procedures offering new opportunities for space industries. For example, the development of SpaceX is linked to the attribution of Dragon vehicle launches within the COTS program.

The reshuffling of US space policy during the twenty-first century has initiated a movement for the entire space sector. It has fueled the interest of a new breed of entrepreneurs from the information technology industry which have renewed approaches to space (Weinzierl 2018). The “new space economy” sums up these individual and corporate investments which have taken place during the last decade. We can list a series of key characteristics which can help us to better understand the specificities of this “new space.”

The first characteristic is the individual dimension of these new companies. Elon Musk (SpaceX) and Jeff Bezos (Blue Origin) represent the most popular and iconic examples of successful IT entrepreneurs who decided to invest in space technologies, with a mix of business plan and grand vision encompassing the future of the world and space exploration. Richard Branson, Robert Bigelow, and Sergei Brin can also be cited for their investment in space. These entrepreneurs are often operating not only as investors but appear to be extremely passionate and knowledgeable, somehow true space geeks, and also directly take part in the technical management of their enterprises (Lewy 2018). They also bring a specific IT business culture, with rapid innovation management processes and important investment capacities. Last but not least, they foster venture capitalism within the space sector, where space start-ups are following the trends we’ve already seen in the tech sector. To sum, we can see a “silicon valley” trend investing the space sector, which helps reinforce this perception of a “new space.”

These trends represent a kind of inbreeding of the space sector and the tech sector. The space industry can rely on a longstanding tradition which goes back to World War II, with important public programs driving an effort toward science and exploration but also defense applications. During the last decades of the twentieth century, space applications for commercial services have grown, with satellites appearing as key infrastructures for meteorological, telecommunications, and positioning systems.

Today, satellites are key components of data retrieving, processing, and transmission. We can observe that business models that were once separate now tend to merge under the powerful umbrella of large platform companies which base their model on data harvesting and processing. This is among the reasons why OneWeb, Google, and SpaceX are planning satellite constellations. This evolution is extremely relevant as it affects both the USA and global markets. The first consequence is that US authorities are able to modify their policy for launchers and to attract new investors. Knowing they can count on the sale of a given batch of launchers enables US rocket producers to lower their price for the international commercial market. This gain in competitiveness on the US launching side represents an advantage when compared to other competitors such as the European Arianespace launcher family

(Darnis 2018). Even within the satellite market, the huge demand coming from US public authorities (civilian and military) represents a comfortable anticyclical cushion for US products. Those two factors can be considered historical parameters that can be summarized by comparing the US space budget to the European one (roughly \$50 billion for the USA vs around \$10 billion for Europe), underscoring a clear supremacy on the part of the USA. But this budget gap did not, until now, correspond to different systems: Europeans were more or less following the same sectors and technologies as the USA and could defend the quality of their smaller productions.

The “new space economy” indicates a different trend, a change of paradigm, with an acceleration on the US side, creating a potential integration of the space sector within the tech sector loop. This development could result in important consequences for space worldwide. On the policy side, we can observe an increasing perception of technological competition between the USA and China, and the recent announcement of the creation of a “Space Force” within the US department of defense pursues this path of a growing strategic and technological rivalry between Washington and Beijing. These trends call for a reinterpretation of global security policy, particularly in Europe.

---

## The Transformation of Space Security

During the second part of the twentieth century, space appeared as a limited but key component of defense policies. Historically, the space race took place at the same time as nuclear dissuasion, and space technologies were developed in a parallel and cross-fertilized way: rocket technology was also useful for missiles, and satellite telecommunication and observation capabilities were integrated into the control and command chain of nuclear forces to do things like transmit orders to submarines or to define targets. Space technologies were integrated within the infrastructure of dissuasion. This is also the reason why those issues had a limited impact in Europe, with the remarkable exception of France pursuing nuclear strategic autonomy and developing some space defense tools from the mid-1970s (Nguyen 2001).

The Balkan conflicts of the 1990s represented a wake-up call for Europe: in strategic terms a conflict was taking place on European soil after decades of peace. Technically, this conflict showed that the US could dispose space-based capabilities for data gathering (Earth observation satellites) and transmission (communication satellites) that were lacking in Europe. Space technology appears to be a key enabling infrastructure for defense. This is the reason why after this conflict, several EU members decided to increase (France) or create (Italy, Germany) space capabilities for security and defense. From the 1990s up to the first decade of the twenty-first century, these “space services for defense and security” paradigm operations like Balkan conflicts or more recently the French intervention in Sahel (Serval, Epervier, and Barkhane operations) confirm the need for space capabilities to be able to project forces abroad. Indeed, space technologies have become key to provide continuity to the command, control, and information chain but also to meet the growing needs in

terms of data bandwidth and also due to the expanding use of computed data-based systems such as drones. This security provided by space also had applications within the European Union with an increasing use of space-based infrastructures for security and safety applications. The launching of Galileo, an EU space infrastructure for navigation (Barbaroux 2016), is quite significant for this issue of security. One of the main reasons for this program was to provide positioning services for the citizens, with the aim of fostering the development of an important application market. This program has been strongly advocated as a civilian one, also to comply with European Union rules, which at the time carefully avoided the defense realm, a member state prerogative. Galileo has, however, created a Public Regulated Service, PRS, to be operated by public security users, including defense. Furthermore the Galileo program has seen a fierce dialectic with the USA which initially opposed this European Union initiative perceived as a competitor for their Global Positioning System (GPS). The Galileo case represents a significant shift for space security in Europe: the debate started around a program decided and built up as a “service to citizens,” but it quickly triggered side effects about the inherent security applications and the foreign policy debate when dealing with USA-UE relations. To a certain extent, the Galileo case represents one of the strongest cases of European Union foreign policy action. Slowly, space policy is coming out from its “science and service to citizens” box and emerging as a potential strategic multisectoral policy.

A direct consequence of this increasing awareness about space issues has been the will to increase the capabilities that allow monitoring of space objects. The question of space debris, together with space traffic, represents a key issue for the security of systems but also the will to monitor potential hostile space objects. This is the reason why the European Union has launched a Space Surveillance and Tracking (SST) program, an initiative which was started under the umbrella of the European Space Agency in 2008 and then moved to a European Union Consortium in 2012. These institutional changes didn’t accelerate a program which still seems extremely limited and relies on the pooling of national existing capabilities, but with a rather low autonomous investment capability. In the meantime, the US Department of Defense, which is responsible for space surveillance and has an impressive set of dedicated resources inherited from the Navy and Air Force space surveillance system, is planning to open space traffic management activities to private commercial firms. This announcement clearly indicates the rapid tempo of US space policy and the will, even in a DoD-only domain, to further embrace the “new space economy model,” fostering the activity of private firms as a resource catalyzer. US space surveillance is extremely interesting as it reveals the evolution of the concept of space security in a post “new space economy” phase. Historically, space surveillance was, and still is, an important feature of the “space power” game played by the USA, Russia, and lately China, with a leading role of the defense administration, which aims to protect its space assets and be ready to react in case of hostile or accidental problems. This need is still strong, but the opening to the commercial market from the US DoD is a potential big bang, comparable to the NASA COTS policy which turned US policy on launchers upside down with huge consequences worldwide. The opening of space surveillance to commercial activities represents an example of

a potential alliance between public authorities like the Department of Defense (DoD) and tech companies willing to retrieve and manage space data. We can already observe how global information technology platforms such as Amazon, Microsoft, and Google develop their business through contracts with the Department of Defense and other public security authorities. Incidentally, those companies are also developing cutting-edge research capabilities in sensitive sectors like quantum computing or artificial intelligence, while traditionally the DoD was the one that held a leading role in new research. These companies know how to accelerate the technological cycles, and a potential transfer of space surveillance to the private sector could enhance US space domination. This concept of “American dominance in space” was used by President Donald Trump in 2018 when he announced the launch of a “Space Force” and also corresponds to the antagonistic posture adopted by the Trump administration when dealing with China in commercial and technological relations.

Europe has to face a multilevel challenge, which is not only to keep up with US and Chinese investments but also to improve the policy level associated to space both as a security provider and a key component of EU global security.

---

## European Space: A Resilient Model

The European space model is a federalist and somehow disparate one, much like the entire European institutional asset. It corresponds to an original buildup between sovereign countries which chose to create a mixed model while maintaining a strong grip on classic sovereignty tools (taxes, defense, security, etc.) and creating institutions for new common policy objectives. Space has a different history in Europe as its cooperation framework was consolidated in 1975 through the European Space Agency, ESA, an intergovernmental organization which has developed capacities and know-how in terms of management of science and exploration space programs. ESA works under the “juste retour” budgetary principle, meaning that each ESA member will receive a return in workload corresponding to its contribution. This rule has been, and still is, extremely useful in order to convince member states to contribute to the ESA budget, as they are certain of the return obtained. This stable mechanism has helped shape significant space activity in Europe over the entire chain of space technologies, from launchers to satellites and ground stations. Europe is part of the narrow club of space powers together with the USA, Russia, and China, countries able to master the whole set of space technologies. It is therefore remarkable to observe that even if Europe suffers a disparity when compared to the USA, with a budget ratio that is four to six times lower, a disparity that is visible in the number of launches and satellites, Europe has still been able to develop an impressive set of technologies, eventually narrowing or maintaining the gap with the USA. During the twentieth century, European space was conceived as a sectoral policy, with a strong investment in research and exploration and important efforts to develop commercial activities for launchers and satellites, benefiting from public research and development support. There is also the development of a launching facility on the European soil, with the Kourou space base. All these investments might seem

difficult to justify when assessed through expenditures. Still they have allowed Europe to develop a strong scientific and industrial basis and impressive operative know-how. Europe has to rely heavily on other programs (Russian, US) only to send its astronauts in space.

The twenty-first century has seen the European Commission entering space programs. This powerful financial institution has brought new resources for the European space sector but also created a certain level of entropy for the management of programs and institutions. The “*juste retour*” rule represents a disparity with the European Commission which funds projects on a competitive and – officially – nonnational basis, creating difficulties for joint ESA/EC projects. As the European Commission progressively increased its action in research funding, it started to deal with space technologies and a first framework agreement with ESA started in 2004. Since then, relations between these institutions are evolving, but the differences between the two organizations’ rules and membership create a series of frictions even if they both express different versions of the same intergovernmental logic. In security policy, and more precisely space security, the two organizations have different rules. ESA results are bound to its “peaceful purpose” status which prohibits defense activities (Cheli and Darnis 2004). The European Commission has insisted for a long time on the strict civilian nature of its program, with member states being extremely reluctant to have the Commission step into defense. In the 2000s, the “security” issue and the “dual-use” aspects of technologies created a rather blurred approach which was embraced by the European Commission when opening funding for “security research.” Even if ESA did not strictly follow the same opening, it contributed to technological development for dual-use systems (e.g., Galileo and Copernicus). This evolution was confirmed in 2016 when the European Commission proposed a defense action plan, with a consensus allowing the European Union to invest in defense technologies. Today, we can observe that an institutional triangle for space security and defense policy is taking place between the European Commission, the European Defence Agency, and the European Space Agency, even if the outcomes of this institutional dialogue are still somewhat limited.

Since the beginning of the twenty-first century, the European space policy model has entered into a transformation phase. Before this period, it was essentially a dialectic between national agencies and ESA, and security was kept out of this collaboration, as some member states developed defense or dual-use capabilities (France, followed by Germany and Italy). In a way, we could say that during the twentieth century, there was no European space security.

Then, a hybrid period started, with the emergence of a blurred dual-use model that we can observe, for example, within the 6th framework program of the European Commission. Industry played a role in putting a budget for space and security on the Commission’s agenda, as companies wished to showcase and develop space-based technologies for applied security, also with the aim of fostering potential pan-European public demand. The logic of space-based products for security services was elaborated to comply with the strong push of “services to citizens” emanating from the Commission: the global philosophy was to demonstrate that

Europe was useful in citizens' everyday life and would produce returns in terms of development of economic activity. This early 2000 mantra with a strong economic rationale was, for example, pushed in documents such as "The cost of non-Europe in the field of satellite-based systems" (Darnis et al. 2007) published by the European Parliament. Space policy analysts had to take into consideration this economic vision in order to introduce some more strategic reflections about space.

But this "space for services" approach also illustrates the resilience of the European space policy model. It is a difficult balance between public funds and commercial activities. For example, the launcher sector, with the Ariane family lately joined by Vega, has always fought to keep its international competitiveness on the commercial market while being directly subsidized through Arianespace. Lately, this model has evolved with the creation of the ArianeGroup, but the equation is still there. Europe can showcase its excellent launching technology, with an impressive rate of success both for Ariane and Vega launchers, but needs public subsidies to keep the sector alive. This is not a political problem as all space launching powers subsidize their launches. The US agencies, for example, provide batches of launches with a comfortable pricing, an operation which allows industrials to lower their price offer on the commercial market. If European Commission rules were applied to the launcher sector in the same manner as other sectors, the subsidies would be banned, an operation which would, however, undermine European interests in the international competition for access to space. This hesitation about the launching economic model in Europe reveals the lack of strategic consciousness about space. Even though important space countries such as France, Germany, and Italy might agree on the need to maintain capabilities and invest in the launcher sector, it is more difficult to share this view with a more pan-European panel which might produce contradictory considerations between general policy declarations which push for a "reliable and affordable" access to space in Europe and more economic-based thinking with criticism about the loss of a complex institutional model or countries which do not feel the need for domestic launching capability.

The US "new space economy" paradigm is pushing European institutions and companies to react. Launchers have been the first to be concerned, and the new European space vehicles Ariane 6 and Vega C represent an effort to lower costs and react to the market push. But again they are threatened by the rapidity of the transformation of US players, able not only to renew their price and public subsidies model but also to push for technological innovation such as reusable vehicles. This economic and technological competition might have a positive effect on the European players who are pushed to further evolution. It is also creating a moment for space worldwide. The popularity and the grand vision of US space tycoons, such as Elon Musk or Jeff Bezos, Donald Trump's declarations about American dominance in space, and the landing of the Change 4 Chinese probe on the dark side of the moon, are gaining relevance for the space activities worldwide. Media, public opinion, and European decision makers are caught up in debates on space policy which did not exist a few years ago. All this attention is already benefiting to the space sector, with the European Commission and European Parliament announcing budget increases.

The "new space economy" also creates a new paradigm for space activities: once isolated, they are now fully integrated into the data gathering, transmission, and

processing value-added chain, a trend which is not only one of the most promising existing business models but also a key issue in terms of security and democracy, as the control of data is already affecting the economy and citizens' lives. Europe missed the information technology revolution by being unable to compete in the processors' industry and not fostering the development of large consumer-friendly IT service platforms able to play a global role. In Europe, no Microsoft, Google, or even Huawei is coming into being. Space, however, represents a sector where Europe can rely on an impressive set of in-house technology. If satellites happen to be today and tomorrow's key components of the data retrieving chain, it is important for Europe not only to maintain its capacities but also eventually to further invest in a sector which is attracting a huge interest worldwide, being able to benefit from the excellent research, technology, and industrial basis that already exists in Europe. The opportunity to maintain and invest in the whole set of space technologies can also translate into a renewed strategic vision of space security. Space can be a security provider but appears here to be a key component of a renewed global security and strategic vision: the capacity to generate and control data is not only the key to winning business models; it is also a fundamental feature to maintain the democratic order and the rule of law, meaning the continuity and the future of our societies. Space will no longer be a sector limited to extremely competent scientists and technicians but also has to be considered by society as the backbone of today and tomorrow's economic well-being and civilian life.

Those considerations mean that space be a key feature of a global European security strategy, which puts technology and data at the center of its interests. For example, we are already observing mobilization around artificial intelligence, calling for further investment and warning that existing gaps with the USA or China might jeopardize our future. But the call to invest in a sector with low capacity in Europe should not distract us from a different and potentially stronger drive: the opportunity to invest in a sector where we already have decent capabilities and where we have a large research and industrial infrastructure able to easily absorb and transform further investment. It is easier to pour money into a relatively large-sized and extremely specialized sector than to create from the scratch a whole new area. Space activities are well structured in Europe, with strong aerospace engineering and physics programs in universities, specialized master cycles, labs, start-ups, public-funded national research centers, national and European agencies, and a large industrial sector. Still, those industrial capabilities are often suffering because of the lack of demand, for example, in the launcher or satellite domain. The number of European launches is comparable to India, while China and the USA are developing an intense activity. There is a risk of marginalization but also an opportunity to maintain and potentially develop further space capabilities by filling today's research and industrial programs, and the European Union can play a decisive role in this. The road is already paved. The Copernicus flagship program is extremely promising but should be further pursued, also in order to provide a European "secure" source of Earth observation products, able to compete on the market not in terms of price and delivery, easily won by future large-sized constellations, but in terms of reliability and continuity of data, a key issue to develop important markets such as public administration as the Galileo PRS already shows. A functioning high-precision



space surveillance system would also represent an impressive value added for Europe, able not only to control space and to sit at the table of future space policies with other space powers but also to take part in the development of commercial-based space awareness services. Also, space surveillance should attract more decisive funds and organization on the European side. This is a key issue in terms of security where different vetoes are keeping the European Commission from hitting the accelerator.

The European space industry does not represent the same level of flexibility and investment capability as the “new space economy” entrepreneurs: in Europe space groups are often the products of a long history, which gives continuity to the sector but sometimes represents a barrier to innovation. But those industries have shown a remarkable resilience and are able to face further technological challenges. They evolve in a composite world, between partially protected national markets, European public programs, and international competition. It would be dangerous to push for a global reform of those market structures in Europe, as they provide anticyclical capabilities to the companies. However, one key logic is missing, an increased presence of venture capital able to foster new technological developments and products for Europe’s space industry. This mechanism is popping up in some member states, for example, in Italy’s space agency (ASI) which has created an investment fund in partnership with venture capitalists in order to foster space-based start-ups and spin-offs. This is a limited but promising experience that could spread throughout Europe, also renewing the action of public institutions.

---

## Conclusion

European space is today on the front line. First because it is a success story, meaning a solid science and technology sector, where Europe defends its excellence on a worldwide level. But space today is at the crossroads of different emerging policies: the reform of defense and security which no longer considers space as simply a “dimension” or as a specific outcome but more and more as a global enabler, a dimension to be included within the information and information technology sphere to create a whole new strategic approach of space. Traditionally, the strategic relations between the USA and Europe were bounded within NATO. Space was out of this scope, as space did not represent a specific transatlantic security issue and even represented as gap between Europe and the USA since space security didn’t allow for dialogue to take place on some issues.

Paradoxically the fact that the European Union has stepped into space activities with its two flagship programs Galileo and Copernicus has improved the European level in terms of space security. Not only because the small size of member states did not allow strategic thinking about space, France being somehow an exception, but also because of the global foreign policy and security impact that those programs had, with Galileo opening the way. While the European Union often faces criticism about its lack of social dimension and its economic criteria, the research and innovation side is largely praised. The European Commission is providing funds and managing

programs that became key for the European scientific and technologic communities, also compensating the lack of national resources. This means that the Commission plays a leadership role in terms of science and technological policy, not only because of funding but also in terms of regulatory capabilities. In the digital realm, we can observe the very relevant regulatory action performed by European Commission under the authority of Vice President Věra Jourová. This technical capacity to raise data and privacy issues and to engage large IT companies has recently created an original set of powers, while member state administrations and governments lack specialization in that domain and have agendas driven by domestic issues. We can observe a technical oriented regulatory and RD investment model emerging at the European Union level. Space is included within this panorama but suffers from institutional competition between the European Space Agency, member state agencies, and the European Commission. The European Commission is the latest player in the game and strives to treat the space sector like other technological and RD issues. The space institutional legacy and know-how lie instead in the hands of the European Space Agency, an international organization whose membership and rules differ from the European Union. As ESA represents precious know-how in terms of project management and space science, it is counterproductive to adopt an aggressive position toward ESA, for example, with a Commission aiming to unify all the space activities under its umbrella and rules. ESA can have a leadership role in research and development for space programs but can also boost its already existing capabilities in terms of Earth observation data management, also considering security issues such as the nature of the data and the need to control and eventually restrain its use.

The European Commission, on the other hand, seems better fitted to ensure the coherence of space policy with information technology and data policies and regulatory issues in a cooperative versus sovereign international technology framework. The EU already has experience with the Galileo frequency negotiations with the USA and is dealing on a day-to-day basis with international IT platforms in order to regulate their business in Europe, with a particular focus on citizens' rights and privacy but also having in mind the development of its antitrust action. Coming from a commercial policy culture, those skills today contribute to a strategic vision which shapes the European position toward non-European companies and States. This is indeed an illustration of an incisive global strategy that can be further developed and pursued within the space sector. The American "new space" example indicates a fantastic acceleration between the reforms of a very robust public demand and the breeding of space with a California-style technological culture. Europe can count on excellent capacities and resilient institutions, with a political consensus often disconnected from central organs such as the European Commission: member states still represent the center of European democracy and for space policy; they are the first and eventually the main level to be involved in key political decisions. This is a rather complicated system, where each member state evaluates its return before making a decision, a reality which helps validate the "juste retour" ESA model. The future of European space policy will have to navigate between those two rocks: member states that are often obsessed by the national justification of their investments which, for space, can only be conceived within an international cooperative

framework and a European Commission which may be a potential game changer for space, with the capacity to enhance space policy within information and data global policies. Within this framework, there must be room for business models in Europe that can imitate some of the US models where public institutions are increasingly buying space capacities, leaving the private sector to deliver an “all inclusive” offer, and eventually opening public resources to commercial activities in order to enhance the system output. If we consider space surveillance as one of the hottest topics for space security, then the somewhat clumsy European consortium could support a strong reform if not a complete revision like the creation of a flagship program to develop a model able to deliver effective monitoring capabilities comparable to the US, Russian, or future Chinese ones. A key condition for the success of a future EU Space Surveillance operational program lies with member states: as surveillance information needs security management, a mechanism like the Galileo security system and procedures, including a Galileo security center, should be developed to ensure the compatibility of a EU Space Surveillance program together with MS security needs. The legacy of existing national systems, mainly radars, appears today as an obstacle as they trigger conflicts in terms of sharing of resources, investments, and ownership between Member States consortium members. A potential flagship program could put an end to these disputes, with the intent to create new capabilities from scratch. This could be developed through contracts with private partners and technical institutions, leaving defense ministers and their assets out of the loop, or proposed through a company consortium. If we agree that global space security must climb higher on the European agenda, then it is important to think in terms of new investments able to mobilize European resources and capabilities and rise up the level of Europe in the world. Space surveillance could just be the next big thing for Europe, if we move on from the current situation contaminated by legitimate, but contradictory, national interests.

---

## References

- Barbaroux P (2016) The metamorphosis of the world space economy: investigating global trends and national differences among major space nations' market structure. *J Innov Econ Manag* 20(2):9–35
- Cheli S, Darnis JP (2004) Towards a European space strategy?, *The International Spectator*, 39:103–114
- Darnis JP, Gasparini G, Pasco X (2007) *The Cost of non-Europe in the Field of Sattelite Based Systems*, European Parliament Study, Brussels, 75 p
- Darnis JP (2018) Access to space, challenges and policy options for Europe, IAI Commentaries, 16/18. <https://www.iai.it/it/publicazioni/access-space-challenges-and-policy-options-europe>
- Lewy Stefen W, 15/10/2018, JEFF BEZOS WANTS US ALL TO LEAVE EARTH—FOR GOOD
- Nguyen A-T (2001) Les échanges technologiques entre la France et les États-Unis: les télécommunications spatiales (1960–1985). *Flux* 43(1):17–24
- Pasco X (2017) *Le nouvel age spatial, de la guerre froide au new space*. CNRS, Paris, 192 p
- Sehovic I (2018) *The NewSpace race: the private space industry and its effect on public support for NASA funding*, working paper, March 2018, 52 p, available at [https://www.academia.edu/36133518/The\\_NewSpace\\_Race\\_The\\_Private\\_Space\\_Industry\\_and\\_Its\\_Effect\\_on\\_Public\\_Support\\_for\\_NASA\\_Funding](https://www.academia.edu/36133518/The_NewSpace_Race_The_Private_Space_Industry_and_Its_Effect_on_Public_Support_for_NASA_Funding)
- Weinzierl M (2018) Space, the final economic frontier. *J Econ Perspect* 32(2):173–192



# Political Economy of Outer Space Security 75

Vasilis Zervos

## Contents

Introduction .....	1512
Security Dimensions and Challenges in Space .....	1513
Economic Background .....	1515
Industry .....	1515
Trade Balance Effects and Atypical Patterns of the Aerospace and Defense Sector .....	1521
Wider Economy .....	1527
Commercial Space as a Space Race Catalyst .....	1528
Political Economy and Security in Space: Institutional Dimensions .....	1529
Conclusions .....	1532
References .....	1532

## Abstract

As human civilizations increasingly explore, utilize, and compete in space, the man-made security challenges are evolving and the strategies and political economic rationales become increasingly relevant for analysis. Sustainability and efficiency call for exploitation of static economies of scale and scope in space industries and services, yet the trade-offs in control, governance, and dynamic innovation point towards autonomy and oligopolistic structures with overcapacity. The economic sustainability becomes a key element of the dynamic pursue of space policies and objectives at national and partnership levels. In the latter case, specialization and its implications for the wide economy through externalities and indirect effects receive increasing attention as space becomes contested, congested, and competitive. Notwithstanding the fact that they are largely government controlled, aerospace industries play a crucial role in trading patterns. Hence, they can be considered a fiscal government spending element similar to

---

V. Zervos (✉)

University of Strasbourg and International Space University (ISU), Strasbourg, France

e-mail: [vasilis.zervos@isunet.edu](mailto:vasilis.zervos@isunet.edu)

defense expenditure. The country specializations and their evolution in commercial markets and alliances are focal points in the current global trade policy paradigm shifts, affecting performance and evolution of space programs and industries. The analysis concludes with the ever-increasing role of regulation and relative power balances across nations, companies, and terrestrial-air-space systems especially for telecommunication applications.

---

## Introduction

Outer space security historically was shaped as a concept during the post-WWII period with the space race focusing on hardware/space assets and weaponization. The maturing of relevant technologies and dissemination of space capabilities to levels whereby undergraduate engineering students are involved in designing and developing nanosatellites and space-proven software and hardware leads to the sustainability agenda evolving at a rapid pace for the future. Sustainability refers not only to manufacturing and knowledge-developing space-based applications and systems, but also to the economic model that reduces costs and augments relevant value to sustain national space industries. This has been critical since the Cold War period that led to shaping of specialization within alliances of overall space support insofar as both civilian and security capabilities are concerned. As space becomes more economically focused through time, such specialization brings forth commercial competitive pressures among allies and questions the initial specialization allocative principle. Thus, Europe, for example (but similar arguments could be made for other allies like Japan, or ex-Soviet Union countries), for several decades has been actively pursuing the objective of space autonomy and commercial competitiveness within the western alliance, despite the US leadership since the early days and the resulting security inter-alliance specialization.

This framework has implications for geopolitical dynamics and partnerships, for efficiency and duplication, but also for the space race “proxied” by national space industrial competition. The support of private-owned enterprises as the space industrial integrators has long (since the 1990s) been employed in the West as a champion of competitiveness in commercial space markets. Leaner, streamlined enterprises without the burdens of disclosure of information and profit assessment by shareholders have emerged. These enterprises are supported at large by high net worth individuals attracted by space and investing through self-developed, financed, and assessed businesses. Ambitious plans of mega-constellations of telecommunication and other application satellites are being financed and developed avoiding business risks experienced with the post-Cold War period when shareholders were exposed to opaque novel space technological operations (Iridium as a characteristic example and others). The “new space” 2.0 thus is based on private initiatives and involves massive investments and production of smaller yet effective satellites in large constellations. The public sector endorses nationally controlled initiatives in this direction as it provides a sustainability of operations and low budgetary appropriations cost not only with regard to the economic resources and organization but also

with regard to industrial scale capability to replenish and mitigate against man-made and natural risks in the perilous space environment. However, the security aspects and market failures associated with space and the overcapacity are expected to lead to real challenges for a competitive market framework and pose real threats to economic and physical sustainability of space resources.

The next section focuses on the background of the security challenges in space, the trade and industrial dimensions, as well as the new space initiatives and their implications for the evolution of space systems and security aspects.

---

## Security Dimensions and Challenges in Space

A space race whereby multiple nations and alliances are involved is ongoing with accelerated pace as new space powers and capabilities develop. Space faring nations develop space branches in the armed forces either integrating aerospace and outer space defense (Russia), or formulating a space force as a separate branch. The case of the USA as the leading space faring nation has characteristically led to a paradigm shift through the evolution of the Pentagon into a Hexagon, to incorporate by 2020 a space force and associated command (DoD 2018: 7). (The structure of the DoD is thus planned to change from one incorporating five branches of the armed forces into a six-branches one with the addition of the space force, by 2021.)

A popular space community say goes along the lines that if one was to lay down the reusable vehicles reports and projects, they would reach the moon. Despite the hyperbola of this statement, space saw limited breakthrough developments in terms of technologies since the end of the Cold War, while numerous studies for ambitious space programs were created, but few going beyond initial paper stages. Commercial considerations and applications grew substantially as the post-Cold War world enjoyed the (space) peace dividend in the form of a multinational space station (ISS), precision in positioning services (removal of selective availability from NAVSTAR/GPS), high resolution imagery and associated applications, telecommunications growth, etc. This peace dividend was the result of technologies that had developed but were reserved for military and associated security considerations. Such safeguarding of technologies and applications are explained by the principle that in the presence of rivalry, it is the relative position that matters, unlike commercial (competitive) considerations that are assumed to rely on overall improvement of positions (Zervos 2011). Thus, selective availability ensured a significant divergence between civil-signal quality and military-signal quality and associated characteristics. Historically though, there have been security threats and military considerations that boosted space technologies development, starting from the very beginning (A4/VII WWII missile) and throughout the Cold War period.

Security is, so far as its space components is concerned, classified along two major areas:

- Nature related
- Man related

Nature-related security threats incorporate elements such as near-Earth orbit threats (asteroids), or solar activity and space weather. On the other hand, man-related elements are of a strategic nature, meaning that they focus on the relative position of agents within a rivalry framework. The USA, for example, identifies the following specific strategic areas of a growing “contested and congested” space environment (see USAF 2013; DoD 2018: 5):

- Nuclear forces
- Cyberspace
- Command, control, communications, computers and intelligence, and surveillance
- Reconnaissance (C4ISR)
- Missile defense
- Joint lethality in contested environments
- Forward force maneuver and posture resilience
- Advanced autonomous systems
- Resilient and agile logistics

Space is considered a strategic domain, similar to nuclear and other WMD (weapons of mass destruction) technologies. This is because space is a major enabler and multiplier in networks (one could draw a parallel with water, electricity networks of vital importance), while at the same time, it is borderless and unregulated by treaties constraining dissemination of relevant satellite and launcher technologies, despite their inherent dual-application nature. Historically, its specific characteristics have served as both a multiplier of force and a peace-through-verification function. Dissemination of technologies, despite being unregulated by treaties, is a major element in strategic security aspects and analysis, in view of the relevant position principle. Thus, export controls exist on a global scale for trade in related items, while an illustrative example of its significance was experienced in the aftermath of the collapse of the Soviet Union, as the USA implemented policies of transfer of resources and collaboration largely to avert a chaotic dissemination of the Soviet advancements (Harford 1997). Clearly therefore, in a world whereby military alliances like NATO are critical for security, the inter-alliance specialization is of particular importance for stability, coherence, and economic (trade) profiles of participating nations. Consolidation in space and the pooling of resources to avoid duplication of R&D and enhance benefits have been dominant reasons behind the creation of space agencies like National Aeronautics and Space Administration (NASA) or the European Space Agency (ESA) at national and regional level. (The early development of space capabilities was characterized by strong competition not only at institutional but also at personality level and led to consolidation at agency level to avoid costly duplication in R&D (see Harford 1997).) Interdependence is also frequently seen as a contributing factor for club, or alliance stability, which implies specialization distributions. At the same time, however, this is an unstable mechanism as countries develop not only multidimensional evolving security policies but also as economic considerations reflect such specialization. The following

section examines the systemic interdependencies by focusing on the industry and its structure-conduct and performance link to public security and defense.

However, beyond the inter-alliance specialization and resulting strategic dynamics, dissemination of space capabilities leads to a “rush for green pastures” approach. This is reflected in two dimensions, the one is the orbital level and the second is the celestial bodies’ level. To avoid conflict over natural resources associated with space, the International Telecommunication Union (ITU) established since the beginning of the space-based telecommunication systems a GEO-orbit and frequency allocation mechanism that employs the principle of equality, rather than first-come. The Cold War-controlled environment has been exchanged for an environment of seemingly free commercial competition and exploration, whereby constellations of thousands of small satellites are planned and materializing. Such constellations are developed within national industrial frameworks and are compatible with security concerns as they sustain technology and production lines supporting responsiveness and ensuring rapid replenishment of assets/capabilities in case of conflict (see later section and Butler 2015). At the same time, such constellations and the required vital space they require for seamless operations lead to a contested and congested outcome across a lot more than the geostationary orbit (USAF 2013). High capacity outcomes may benefit civil users but may also exacerbate security concerns associated with earlier projects like Iridium, whereby national service providers and authorities would see restricted economic returns, while experiencing dependence for relevant telecommunication security.

---

## Economic Background

### Industry

The space industry is subject to economies of scale/scope; market failure is present at several levels through the aforementioned cost and market characteristics leading to infant industry arguments but also due to the strategic economic nature of the sector (airbus vs. boeing and the launchers market analysis).

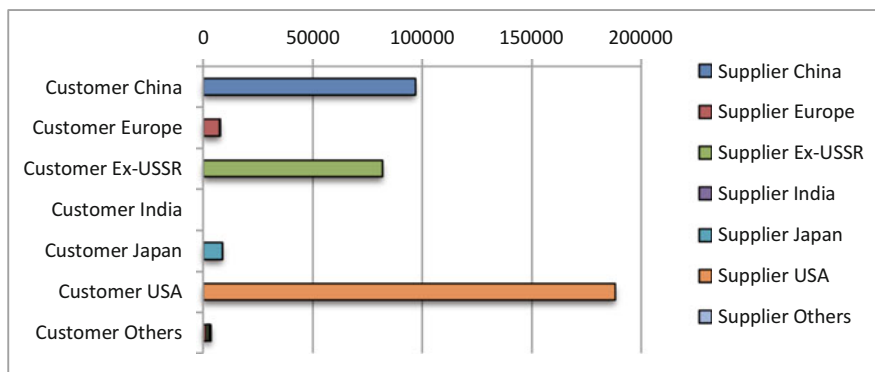
The Research & Development (R&D) intensity of the space sector is quite high compared to other manufacturing and high-tech sectors. In the United Kingdom (UK), the R&D intensity of the sector is estimated at 8.1%, which is higher than sectors such as programming and telecoms but lower than the pharmaceuticals sector. Compared with the UK average, the space industry spends 6.5 times more on R&D in value terms (HoC 2017). Other studies offer estimates for the Italian industry of R&D intensity of 14% for the space industry versus 3–4% for the space services sector (compared to 11% in aerospace; 4–5% in high-tech sectors and less than 1% in manufacturing; Graziola et al. 2011). The undoubtable relatively high R&D intensity is due to the high R&D requirements but also due to the limited production levels (compared to car manufacturing or defense manufacturing), as most programs are of a customized/limited production at national level nature.



This is clearly illustrated in the military satellites case whereby national considerations and preferential treatment are dominant. As Fig. 1 reveals, in military space, satellites are “home made” on a global scale. This phenomenon is not only due to demand side aspects whereby countries select their home industry to enhance its scale and scope economies, as well as the security factors, but also due to the supply side through export restrictions.

These export restrictions serve to safeguard technologies, as trade can rapidly diminish technological gaps limiting the scope for global trade openness in the sector. An anecdotal illustration of the strategic nature of the space sector emerged during a commercial space dispute whereby a US company filed a complaint with the US administration over European free-trade violations and associated practices in launching service provision through the heavy subsidization of the European launch vehicles. This took place during the Cold War era in 1985 when a US company (Transpace Carriers Inc.) brought a legal case against ESA and its member states to the attention of the President of the USA claiming among other things that Arianspace faced a protected home market and this was violating the US Trade Act of 1974. The case was dismissed largely on the grounds that the US public sector applied similar protective processes to its domestic space industry (using provisions related to “Buy American Act” and others):

Based on a petition filed by Transpace Carriers Inc., (TCI) the United States Trade Representative (USTR) initiated an investigation on July 9, 1984, of the European Space Agency’s policies with respect to Arianspace S.A. Arianspace is a privately owned company, incorporated under the laws of France for the purpose of launching satellites. Arianspace’s shareholders include the French national space agency, and aerospace companies and banks incorporated in the ESA Member States. The petitioner alleged that 1) Arianspace uses a two tier pricing policy whereby Arianspace charges a higher price to ESA Member States than to foreign customers; 2) the French national space agency (CNES) subsidises launch and range facilities, and services personnel provided to Arianspace; 3) the French national space agency subsidises the administrative and technical personnel it provides to Arianspace; and 4) Arianspace’s mission insurance rates are subsidised. In addition to

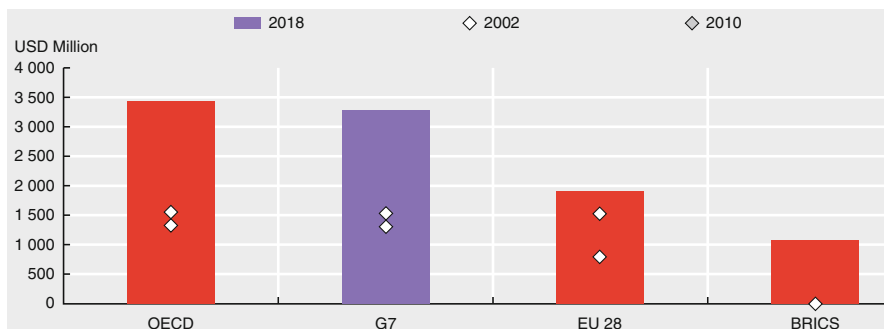


**Fig. 1** Military spacecraft markets by customers and suppliers for selected areas 2013–2017 (Mass-kgs). (Source: Copyright Eurospace/Pierre Lionnet – reproduced with permission)

these allegations the U.S. also investigated three other areas: government inducements to purchasers of Arianespace’s services; direct and indirect government assistance to Arianespace; and Arianespace’s costs and pricing policies....Pursuant to Section 301(a) of the Trade Act of 1974, as amended (19 U.S.G. 2413(a)). I have determined that the practices of the Member States of the European Space Agency (ESA) and their instrumentalities with respect to the commercial satellite launching services of Arianespace S.A. are not unreasonable and a burden, or restriction on U.S. commerce. While Arianespace does not operate under purely commercial conditions, this is in large measure a result of the history of the launch services industry, which is marked by almost exclusive government involvement. I have determined that these conditions do not require affirmative U.S. action at this time. But because of my decision to commercialise expendable launch services in the United States, and our policies with respect to manned launch services such as the Shuttle (STS), it may become appropriate for the United States to approach other interested nations to reach an international understanding on guidelines for commercial satellite launch services at some point in the future. (Reagan 1985)

In terms of trade patterns of space goods, for spacecraft and launch vehicles, export performance is led by OECD countries and reveals upward trends as more and more countries become involved in space technologies and applications initially through trade. Figure 2 from OECD 2019 compares exporting snapshots for 2002, 2010, and 2018 illustrating relative export positions of groups of countries (constant USD) and revealing positive trends.

With reference to the breakdown of export performance by country in space goods, France appeared the leading exporter in 2018 data with nearly 28% of the total, followed by China (22%), the USA (20%), Japan and Germany at about 8% each, and Israel at nearly 6% (OECD 2019, using ITCS classification 7925 – spacecraft and spacecraft launch vehicles). For time comparison purposes, it is worth noting that the HS 880250 figures reveal that in 2017, the US exports were



**Fig. 2** Space export performance of selected areas. (Data source: OECD 2019: 31). Notes: OECD figure is based on UNCOMTRADE database and HS classification coding 880260 that is comprised of spacecraft and suborbital and spacecraft launch systems. (Direct from the UNComtrade database data is unavailable for HS 880250 (spacecraft and launch systems – without inclusion of suborbital vehicles), and there may well exist discrepancies across “as reported” data, with the values for EU28 as a group reported lower than the sum of the countries (no clear indication of consolidation), as well as for SITC 7925 (“as reported” for the selection of countries like USA, China, France, and others for 2018))

slightly higher (USD 1.48bn) than the ones of France (USD 1.72bn) highlighting the volatility of the time series data in view of the institutional nature of trading partners and limited overall values involved (Data source: UNComtrade database).

Europe and France have historically focused on an export-led model on the grounds that the “domestic” market size is too small to support an efficient size of operations of the aerospace industry in general (owing to the economies of scale and scope) compared to countries like the USA.

Trading performance is generally expected to be linked to budgetary appropriations that support and develop space technologies of domestic industries. This is owing to the fact that the space industry is subject to some traditional market failures since the early days such as:

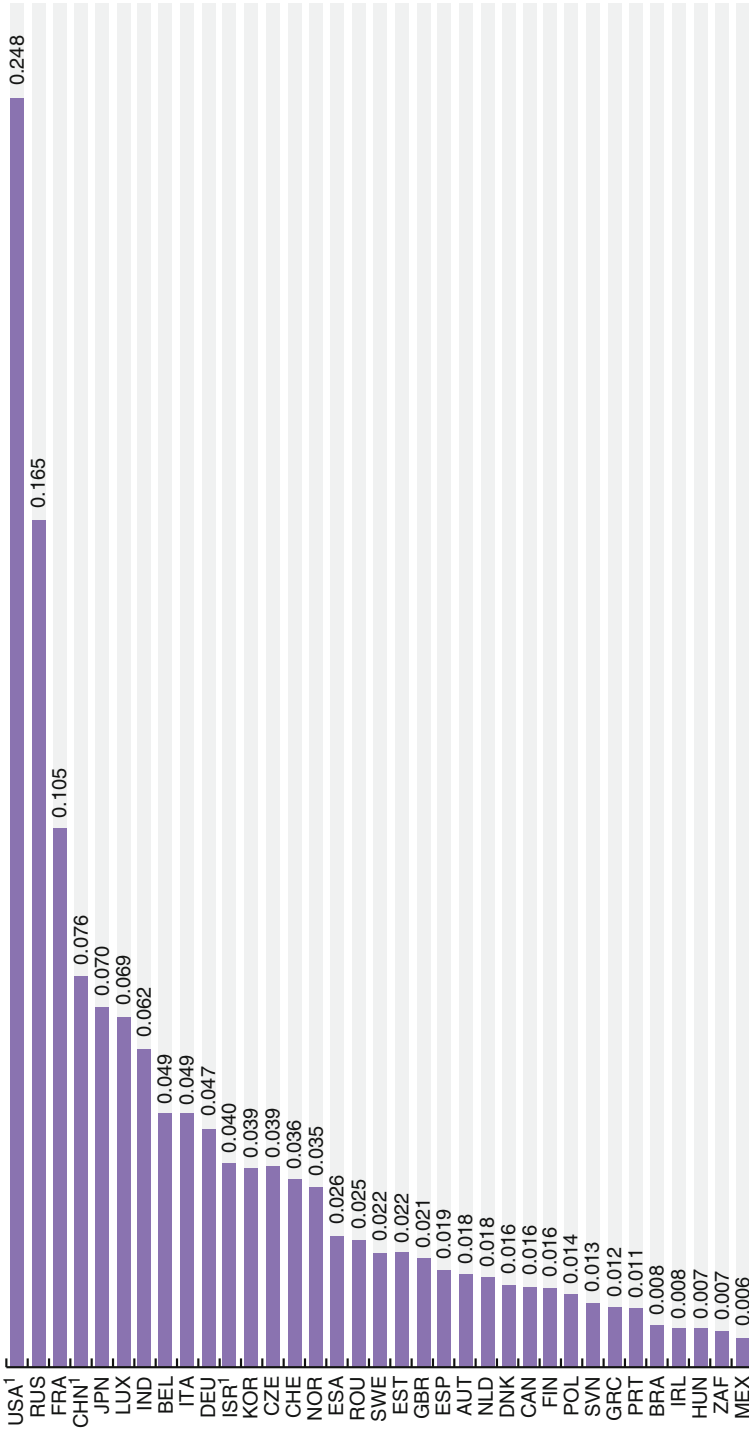
- *Public goods.* The two characteristics of public goods, jointness of supply (zero marginal production costs) and non-excludability are found in the provision of goods, such as national security and defense based on strategic space capabilities. Prominent examples are the space-based defense applications of earth observation (EO), navigation, and telecommunications, vital elements of national defense capabilities of NATO and Warsaw Pact countries during the “Cold War.” Despite variations in the supply of such goods across the NATO alliance, for the country that owns space assets with defense and security capabilities, the respective benefits accrue to all its citizens. Beyond the public goods nature of space services by nature of the service itself, there is also public good by convention. An example of this is the geo-navigation and positioning systems, whereby the USA offers a free to users signal along with its protected (encoded) military signals. This means that there is no rivalry and non-excludability (by convention) to the users (Zervos 2018).
- *Natural monopolies.* Where there is decreasing costs, production mode of a good and a sole provider reduces duplication (see later) and is also desirable for security reasons. The use of decreasing costs arguments has been used in the provision of space-based goods by “natural monopolies,” such as telecommunications services prior to the recent privatization of telecommunication organizations in Europe. Prominent examples are the case of the international telecommunications satellites organization (INTELSAT) and international maritime satellites organization (INMARSAT). INTELSAT, the first civil global communications network, was created in 1964, followed by the launch of the “Early Bird” satellite. Prior to the end of the “Cold War” and the commercialization of major telecommunications service providers in Europe and Asia, it was implicitly agreed by its members that INTELSAT is a “natural monopoly” (Snow 1976, 1987a, b; Rostow 1968) and a procedure has been determined (Article XIV (d) of the Intergovernmental agreement) to establish whether other commercial systems would inflict any “significant economic harm” to its operations. The rapidly expanding size of the global telecommunications market and the large-scale privatization of telecommunications in Europe and the USA led to uncertainty surrounding the continuous non-rivalry to INTELSAT by private systems.

Following increasing competitive pressures, INTELSAT's assembly of parties (shareholding organizations, commercial, civil, and national) decided to restructure the organization and ultimately commercialize it by July 2001. Despite the growth in telecommunication service providers, the significant market concentration and network-economies associated with satellite systems signify oligopolistic markets with economies of scale and scope in operations. This is expected to extend to planned mega-constellations of satellites leading to contested and congested orbital space with potential overcapacity. Overcapacity and the ability to replenish basic operations in case of accidents or hostile operations provide first-mover advantage to space-faring nations whose industry will operate such constellations (See [Commercial Space as a Space Race Catalyst](#)). (See Rostow (1968) for an early policy-economics analysis and discussion on newly developed challenges from space-based telecommunications. Key points identified relate to avoidance of concentration of power and control to the hands of the government or the industry, while recognizing the natural monopoly challenges. The X-inefficiency (innovation factor) and power dissemination forces are arguably operating against the single-natural monopoly solution in a static decreasing-costs sector.)

- *Uncertainty, risk.* The risk associated with new space technology was and is high. As technologies for some space products mature the risk associated with such applications decreases and commercial markets are more willing to finance and support them. Telecommunications organizations and firms can thus afford to insure against a variety of risks the satellite and the launching process are subject to.
- *Externalities.* Positive production and consumption externalities, as well as spin-offs. Social cost avoidance from using, for example, geo-positioning systems like GPS on a popular basis saving on consumers' transportation costs, congestion and pollution costs, and others. Spin-offs from space technologies and production cost reduction for industries employing precision in location, but also timing information, along with technical progress associated with space goods (Zervos and Siegel 2008).

As a result of significant market failures, especially with regard to the positive externalities, public goods nature, and security considerations associated with production and control over national space assets, space-faring nations develop indigenous capabilities reflected in budgets. In view of the non-tradable nature of most space goods, international comparisons based on monetary value pose challenges of accurate reflecting relative positions and capabilities.

In this context, budget information such as OECD (2019) provides relevant estimates (Fig. 3) of relative budgetary appropriations indicating prioritization that are useful in indicating relative country positions rather than absolute numeric comparative statistics. (Clearly the downside of using percentage ratios is that small-sized budgets may well lead to low overall scale of programs and industries for smaller countries.)



**Fig. 3** Space spending as a percentage of GDP. (Source: OECD 2019: 24)

### Trade Balance Effects and Atypical Patterns of the Aerospace and Defense Sector

Space versus aerospace when considering trade patterns overall performs quite interestingly. In aerospace, especially civilian commercial airliners, the dominant companies (namely Airbus and Boeing) are largely unchallenged and their export performance act as balancing forces in otherwise unbalanced trade patterns, especially with countries like China, space (military) as we saw has a different behavior. Figure 4 reveals that the USA experiences significant overall trade deficits that are persistent in recent decades.

The economics and overall rational of this global trade pattern is a point of controversy in terms of policy and trade agreements on a global scale recently, yet it is worth noticing that aerospace acts as a balancing sector with regards to specific countries such as the USA and China. Figures 5 and 6 reveal that the USA’s aerospace balance has the opposite trend of the overall trade balance, mitigating somewhat overall deficits.

As Fig. 7 further illustrates, US (aerospace) exports are specifically significant with regards to China, which specializes in non-aerospace sectors in terms of export performance.

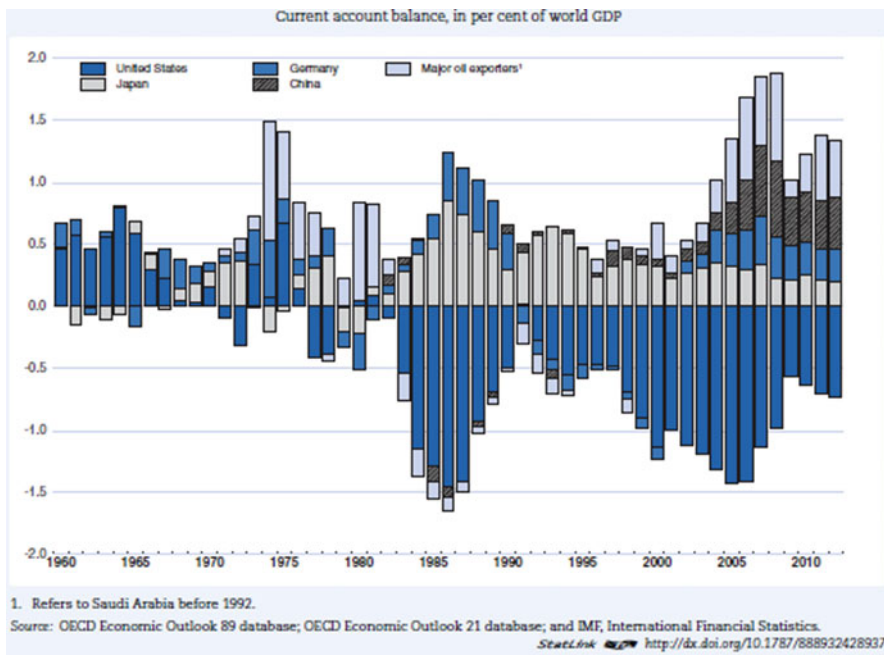


Fig. 4 Global trade patterns. (Source: OECD database)

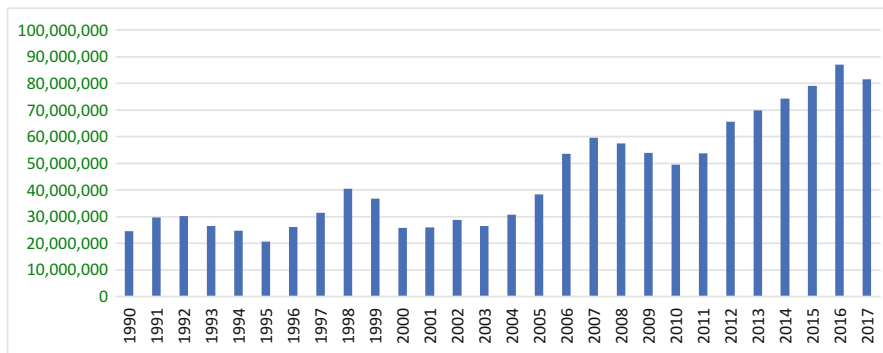


Fig. 5 US balance of trade for aerospace goods. (Source: OECD database)

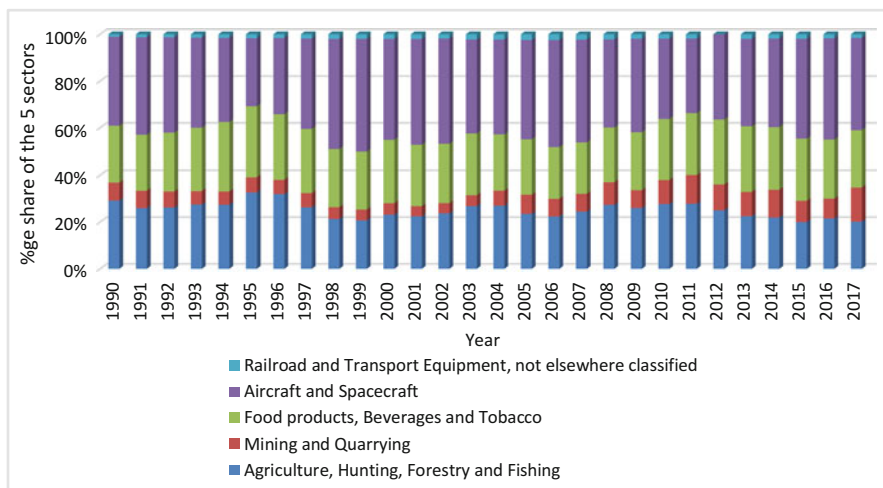
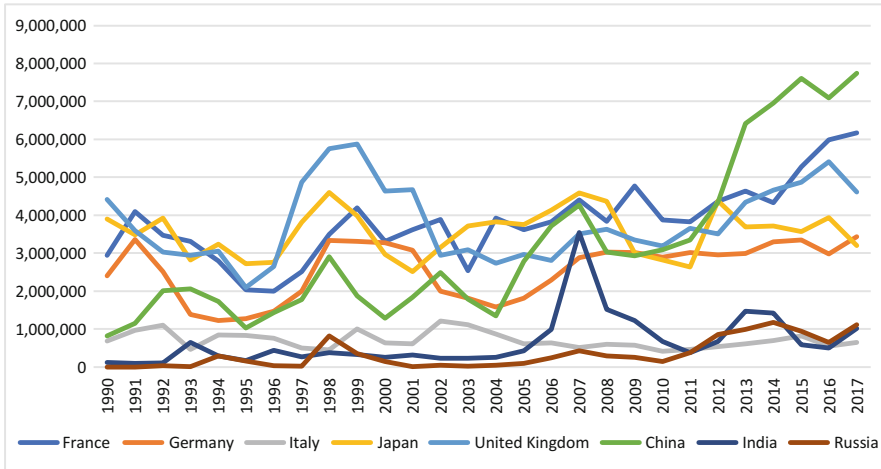


Fig. 6 US exports sectoral distribution. (Data source: OECD database)

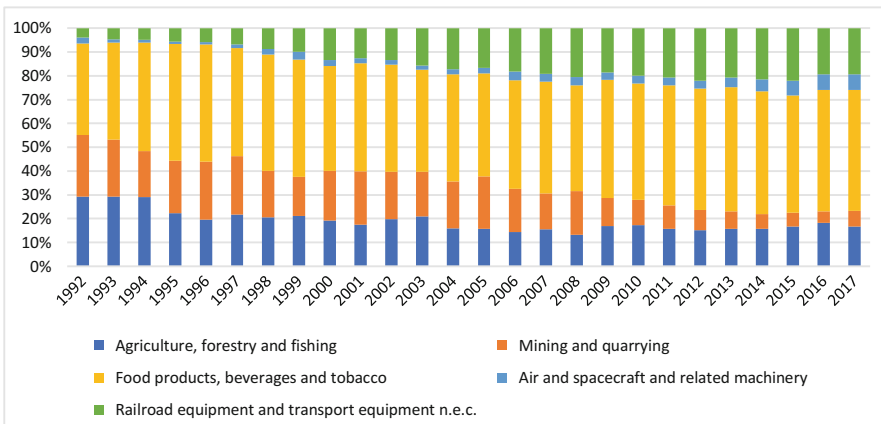
The Chinese export performance is gradually shifting towards the aerospace sector, though the trade specialization overall is focused on alternative industries (Fig. 8).

The same is seen when considering other Western nations like France and the UK that are traditionally considered as underperformers in trade balances. By examining trade balances overall and comparing them to the sector of aerospace goods and services reveals that for major trade performers like Japan, China, the aerospace sector acts as a balancing element compared to countries such as the USA and France (Figs. 9, 10, 11, and 12).

Clearly, specialization plays a key role in trade patterns. In addition though, political aspects, such as heightened tensions and sanctions, seem to impact upon trade patterns and benefit (in relative terms) the aerospace industry. The trade pattern



**Fig. 7** US exports in aircraft and spacecraft (constant values). (Data source: OECD database)

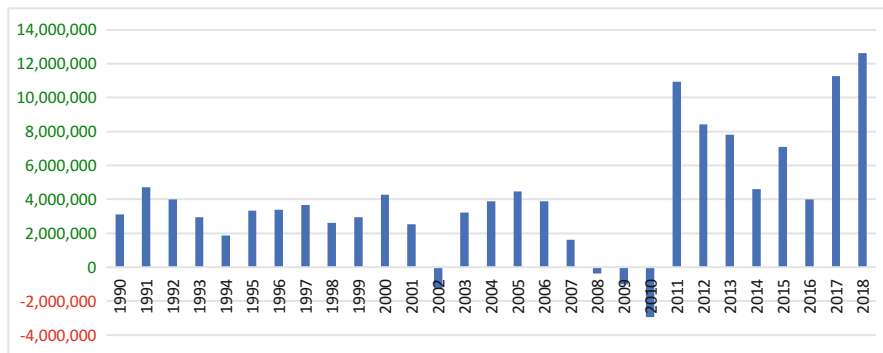


**Fig. 8** Chinese exports specialization. (Data source: OECD database)

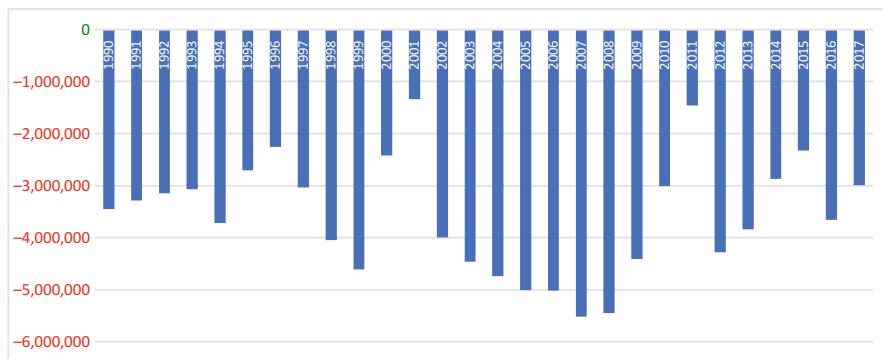
changes from the USA and France to Russia illustrate this in Figs. 13 and 14 as rising tensions and sanctions seem to result in a notable increasing aerospace share of overall export performance.

Export restrictions play a significant role in trade patterns and reveal a significant trade-off between short-run sales and maintaining of technological edge as perceived by dominant powers like the USA. Thus, the domestic “demand” for space-related security is very high in the USA, but the same can be said of other major space powers as they themselves invest in space unilaterally when it comes to critical space technologies, while they also do not release technologies on par with other (exporting) sectors. This is compatible with the dual-use, as well as the security strategic nature of space. Space capabilities are conceivably on-par in

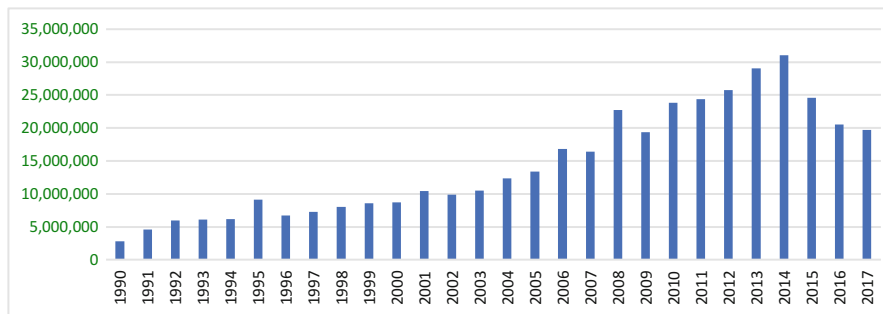




**Fig. 9** Balance of trade in aerospace goods for the USA. (Data source: OECD database)

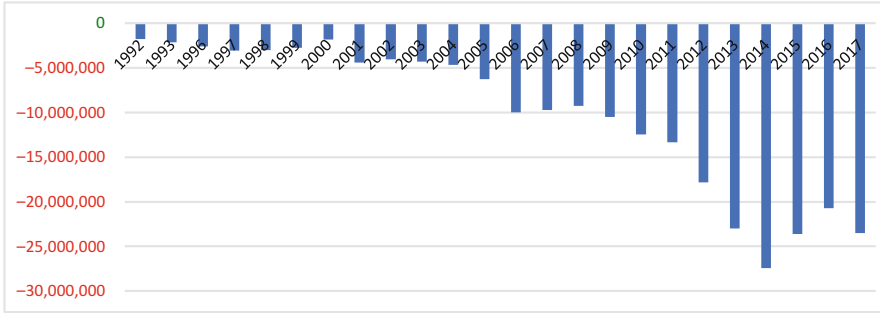


**Fig. 10** Balance of trade in aerospace goods for Japan. (Data source: OECD database)

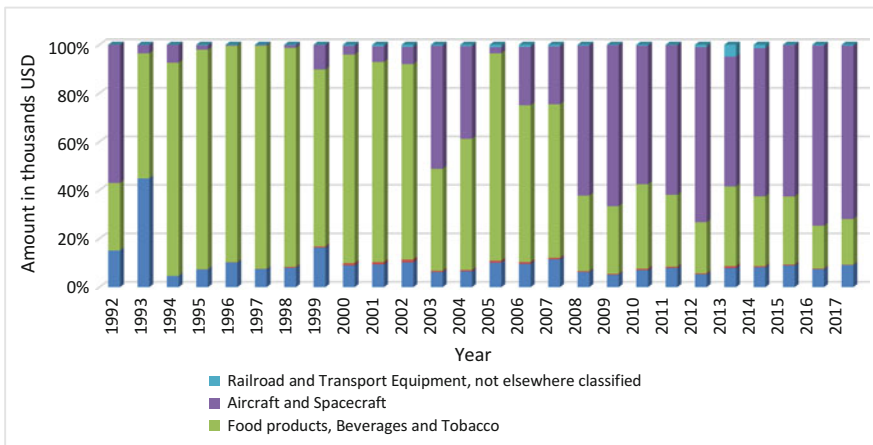


**Fig. 11** Balance of trade in aerospace goods for France. (Data source: OECD database)

terms of their security special “weight” with nuclear weapons but not bound by any treaties in terms of their development. The aerospace goods and services trade patterns are clearly not applicable in the case of military satellites as seen earlier in Fig. 1.



**Fig. 12** Balance of trade in aerospace goods for China. (Data source: OECD database)



**Fig. 13** Sectoral breakdown of French exports to Russia. (Data source: OECD database)

Industries subject to economies of scale and scope are long considered as strategic on the grounds that they exhibit significant industrial consolidation, frequently resulting in national champions that may collaborate in multinational institutional markets either at the industry or at the government level, while at the same time compete in commercial markets. Figure 15 captures such a framework for the space sector (not unlike the wider aerospace and defense sectors) and the resulting formation of institutional-industrial complexes.

In its simple form, such a framework is depicted by a structure whereby a national industrial champion exists (largely owing to the economies of scale and scope cost characteristics) that must also provide a level of national security in autonomous provision of security-sensitive goods. Such national champions face domestic monopolistic markets, while compete in commercial markets of an international nature.

A further element in this analysis is the nature of the “domestic” government space good or service (defense/security), as they may well constitute in the presence

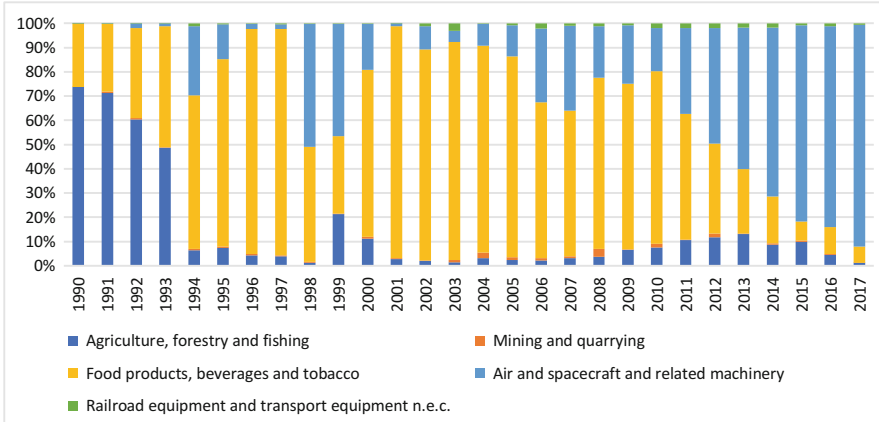


Fig. 14 Sectoral breakdown of US exports to Russia. (Data source: OECD database)

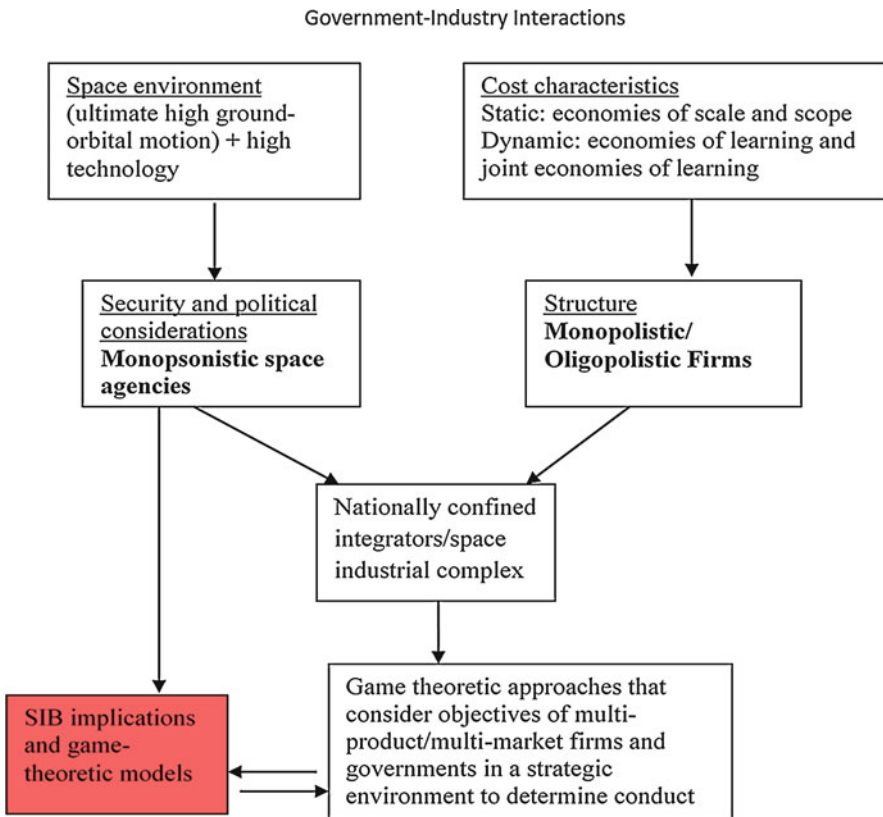


Fig. 15 The space industrial complex analytical framework. (Source: Zervos 2018)

of an alliance public goods. Public goods within an alliance or a research organization are complex goods and services. For example, “security” within NATO would refer to more than a single technological asset (ICBMs) but would require a network comprised of supportive nodes (including assets like GPS, intelligence, logistical support, tactical weapons, NATO localized basis, etc.). Thus, the main provider is seen more as an integrator and less as a vertical integrated entity. There are clear resemblances with supply chains and production technologies where “subcontractors” or lower tier suppliers exist and contribute at different levels. The distribution of alliance member contributions in the presence of economies of scale and scope is of paramount importance for the allocative efficiency.

Furthermore, following an extension of the Balassa-Samuelson framework, where a competitive tradable sector affects the relative wages of the non-tradable sector, tradable-sector specialization and development can have multiplier effects across the economy. This is not only in the presence of global supply chains but also in the case where the specialization follows a collaborative negotiated and agreed approach across partners, as is the case of alliances (NATO), or joint organizations like the ESA. Zervos (2011) shows how in strategic industries where economies of scale and scope co-exist with a tradable and governmental non-tradable sectors (defense), the non-tradable sectors are not only interconnected but can also have an unexpected impact upon the performance of the tradable sector by perverse incentives. That means that the economy with the cost advantage in the non-tradable sector may not see this advantage extended into the tradable sector, since rent-seeking behaviors prevail. This leads to an introverted focus of firms to their domestic lucrative market, rather than the more competitive global one, even though the country enjoys a theoretical cost advantage should its industry decide to capture the global market.

## Wider Economy

Significant externalities and hard to measure security benefits, but also linkages of industry create an atypical environment with significant market failings, but also potential crowding-out owing to the flag-carrier and prestige impact space enjoys.

Previously examined trade balance effects thus do not take into consideration the expected greater impact of space sector manufacturing in terms of spin-offs and multiplier effects, compared to other economic activities from services and elsewhere. In addition, successes in space that have an uplifting impact on society and are associated with flag-carrier effects are hard to monetize, but potentially can have a critical impact on future generations and science and technology developments through time. Thus, it is unsurprising that there have been several attempts to quantify the economic return of space activities, either at the business-planning level for commercially minded endeavors and public-private partnerships or at the micro- (sectoral) and macroeconomic levels (Hertzfeld 2002). There are evidently significant methodological challenges to be considered, notwithstanding the “client commissioned” approach that poses additional challenges to the uncritical adoption

of the results. This has been evidenced since the early US macroeconomic studies by US institutions questioning the relevant methodologies insofar as the value of the findings is concerned. Moreover, the partial nature of the analysis typically falls short of addressing the opportunity cost of appropriations devoted to space. (For a review, see Zervos (2002); regarding business studies optimism, a relevant example guiding public policy in Europe is the case of Galileo (Zervos and Siegel 2008).) On the other hand, the highly important security aspects are by-nature hard to monetize, despite the expected high value to economic activity and society.

---

## Commercial Space as a Space Race Catalyst

The economic background indicates how the commercial markets connect seemingly unrelated monopolistic domestic markets (Zervos 1998). The conduct and performance in commercial markets therefore impacts upon specialization dynamics within security/military alliances in a dynamic environment. Thus, government support for commercial performance may well signal conflict and competitiveness at government and security-levels, especially within alliances. It is noteworthy to observe that trade specialization is thus not unrelated to alliance and geopolitical frameworks. The commercial “new space” environment and aspirations were initially experienced during the first wave of commercialization and following the end of the Cold War (peace dividend applied to space) and led to sobering results (Iridium/mobile space telecommunications), following optimistic market projections of a similar nature to the market estimations with regard to the Galileo system. The newly created space companies, with origins to be found in the support by wealthy space enthusiasts like Branson, Musk, Bezos, and others, utilize capital to develop space technologies with the support of the public sector, but importantly, also seemingly rely on such support as a customer base. The commercial sector is thus government-dependent and nationally bound, perhaps more so than earlier alliances like SeaLaunch. The openness of the post-Cold War in industrial partnerships and exploration of space is therefore replaced by nationally confined considerations whereby the newly sprung enterprises compete on grounds of efficiency with publicly listed companies, focusing on innovative improvements, cost performance, and market share.

Commercial considerations are frequently evoked to equate success at the market share level (measured by market dominance and turnover), rather than a mature, government-independent industry with sound business investment (commercial) criteria. Thus, government-induced investments aiming at generating market revenue may prove to follow a nationally or geographically confined creation approach. The partnership approach utilized in other industries to avoid duplication in R&D and exploit economies of size appears heavily constrained. “Galileo, for example, is likely to have progressed at a much smoother political route, fastest pace and lower costs had the US participation been possible at contractor’s level, in exchange for European industrial involvement on US relevant space projects” (Zervos and Siegel 2008).

## Political Economy and Security in Space: Institutional Dimensions

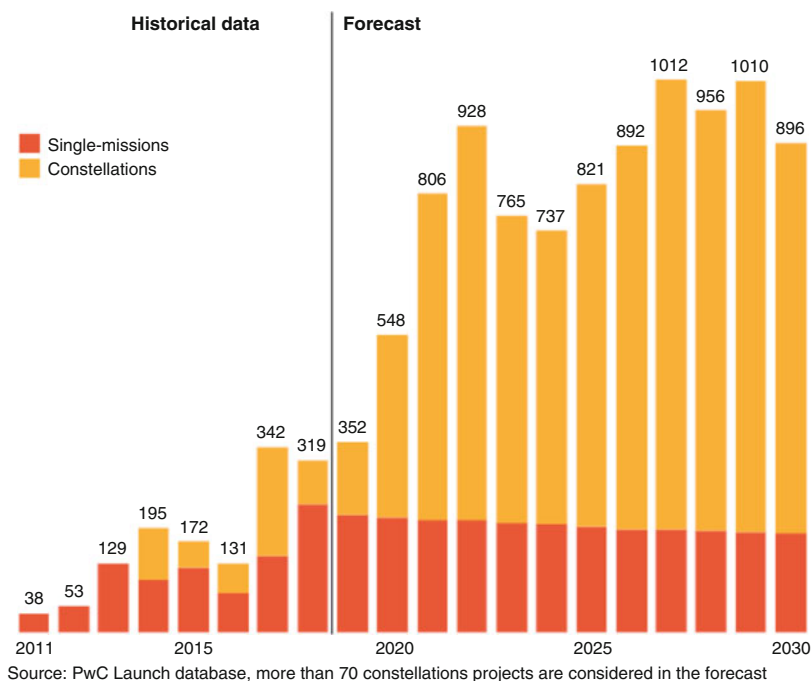
Assuming that the labeled commercial space programs act as an enhancer of conflict in space, they may hinder rather than promote security even with regards to conventional space collaborative programs like NEO threats. This is owing to the fact that the impact of government programs on the commercial competitiveness of participating industry enhances transaction costs and rivalry. Thus, even though rivalry may benefit the industry through duplication of capabilities and globally increasing size and public spotlight (an impact identified since the days of Sputnik-Apollo), it may also constrain the short-run development of projects of common security interest. (In addition, such rivalry may well impact also upon collaboration in flagship programs like the ISS, as well as scientific and exploration ones.) The collapse of the Soviet Union and the resulting hegemonic position of the US diminished the rivalry perceptions between the USA and Russia allowing for a number of commercial and public collaboration, in contrast to the heightened commercial competition levels between the USA and Europe at the time. The rise of China, India, Japan, and others as they develop significant capabilities may well result in the future in relevant initiatives, but it seems that a rules of the road approach for the commercial markets and the conduct of industry/providers in these is a critical element for global sector developments in the future. Clearly, the World Trade Organization (WTO) may be a challenging environment for such developments, hence further research and novel approaches may be developed towards enhancing sectoral growth and security simultaneously.

Even though the WTO is of perhaps lesser concern to space, organizations like the ITU are critical in dealing with spectrum allocation mechanisms as they evolve into continuous liberalization from an initial equitable basis of *global commons* good are more space-focused in their agendas. Thus, the abandoning of the INTELSAT model of globalization of telecommunications and allocation through an early global partnership and governance mechanism into a private enterprise-oriented one is implemented through evolving mechanisms and licensing of orbit and spectrum allocations. The regulatory role is thus increasingly supplemented by heightened monitoring requirements requiring novel institutional arrangements as space is becoming more congested and contested in Earth orbit, but also in potential future exploration specific locations such as Lagrangian points of interest, lunar hotspot ones, or Martian and other celestial bodies.

The explosion of small-satellite constellations largely associated with the advent of global telecommunication services and mobile data leads to multiple levels of contestability and congestion starting from higher atmospheric through to high orbital planes. (The term is used in this context to describe low mass satellites (less than 500Kg mass) that include what is habitually defined as nanosatellites, picosatellites.) The situation is perhaps analogous to the pre-digitization era of remote sensing satellites based on film technology that were used by the USA and the then USSR to observe the Earth and their lifetime extended to the capacity of the film that needed retrieving at the end of each satellite mission (and its end of life), thus resulting in a continuum of launches and disposable film-containing

satellites. Longer lifetime, but small satellites requiring replenishment, and/or servicing are planned to support 5G and other telecommunication systems. As Fig. 16 reveals, there are planned constellations that add up to over 10,000 new smallsats all of which require their vital space in terms of physical proximity of operations and spectrum/interference topology, mitigation, disposal, and replenishment plans that are harmonized on a universal level and require situational awareness and regulatory evolution. In case of business failures, or abandonment of plans, such operational costs and legal challenges may lead to non-simple solutions requiring governments being able to support such instances when licensing and hosting relevant businesses. (It is evident that such industrial and network replenishment national industrial capacity that is economically sustainable is welcomed by the security agencies for countries like the USA. It would be significantly more costly to maintain industrial capacity without exploiting the relevant scale and scope, producing just for military/security purposes along the lines of Operationally Responsive Space (ORS), developed largely in response to the Pearl Harbor scenarios for space assets (Commission 2001).)

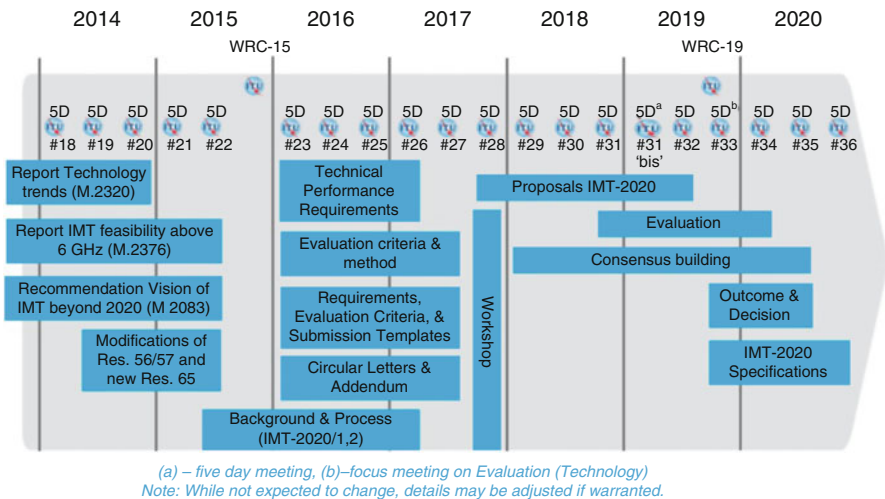
In addition, this new trend is placing a burden upon the ITU's role with physical and spectrum space becoming scarcer and therefore adding the dimension of placeholding, moral hazard, and speculator behaviors. In response, the ITU has tighten up the licensing conditions and implementation requirements by relevant



**Fig. 16** Trends in small satellites (single mission and constellations). (Source: PwC 2019)

enterprises to avoid low-cost reservation of space with lengthy implementation and inactivity periods. The ITU is also faced with scarcity of spectrum as 5G systems and new technologies offer great opportunities for users but also pose challenges on the space/airspace/terrestrial architectures and allocation (as well as uses between telecommunications, science and exploration, and others). The ITU is thus planning following the WRC-19 milestone to establish harmonizing conditions for this multidimensional architecture to enhance order and efficiency in view of the congestion challenges (Fig. 17; Henry 2019; ITU 2015, 2016).

The global reach of such “utility” services raise the issue of governance of networks, safety, and security standards and control of operations. The private nature of such global utilities and the different legal regimes between users and operators are expected to exert force towards multi-stakeholder partnerships, or quasi national autonomous systems. Thus, despite potential economies of scale and scope in operations, it is likely that again there will be overcapacity and multiple systems in place augmenting harmonization and efficiency challenges. A critical challenge, though, for future security lies ahead with regards to the utilization of resources, as technical capabilities increase and disseminate with a rising number of space-faring nations coupled with challenges to the status quo of space resources utilization. The partial application of an ITU-like model for specific space cases may be an option, but it is not clear whether such an option would gather the analogous momentum at global level when dealing with a variety of resources (besides telecommunications/GEO). Moreover, space traffic management faces significant challenges, when compared with the tested aerospace/FIR applications and operability, that may though nullify as technical expertise disseminates.



**Fig. 17** ITU timeframe for regulating 5G. (Source: ITU 2016)



## Conclusions

Outer space security is a multidimensional concept; the most usual direct application is found in near-Earth objects, as well as other natural threats (solar storms and others). However, as humans increasingly explore, utilize, and compete in space, the man-made security challenges are evolving and the strategies and political economic rationales become increasingly relevant for analysis. Sustainable industries and efficiency call for exploitation of static economies of scale and scope in space industries and services, yet the trade-offs in control, governance, and dynamic innovation point towards autonomy and oligopolistic structures with overcapacity. The economic sustainability becomes a key element of the dynamic pursue of space policies and objectives at national and partnership levels. In the latter case, specialization and its implications for the wide economy through externalities and indirect effects receive increasing attention as space becomes contested, congested, and competitive. Space and aerospace industries play a crucial role in trading patterns, notwithstanding the fact that they are largely government controlled, hence can be considered as a fiscal government spending element similar to defense expenditure. The country specializations and their evolution in commercial markets and alliances are focal points in the timely global trade policy paradigm shifts, affecting performance and evolution of space programs and industries. The chapter concludes with the ever-increasing role of regulation and relative power balances across nations, companies, and terrestrial-air-space systems especially for telecommunication applications.

---

## References

- Butler A (2015) USAF operationally responsive space office could oversee next SSA, Weather Sats. *Aviation Week*, February 12. <http://aviationweek.com/space/usaf-operationally-responsive-space-office-could-oversee-next-ssa-weather-sats>
- Commission (2001) Report of the Commission to Assess United States National Security Space Management and Organization. Commission to Assess United States National Security Space Management and Organization, Washington, DC
- DoD (2018) Summary of the 2018 National Defense Strategy of the United States of America. Unpublished, Department of Defense, US
- Graziola G, Cefis E, Gritti P (2011) *L'industria Spaziale Italiana nel Contesto Europeo*. IL Muliko, Bologna
- Harford J (1997) *Korolev: how one man masterminded the soviet drive to beat America to the moon*. Wiley, New York
- Henry (2019) ITU wants megaconstellations to meet tougher launch milestones. *Spacenews*. [https://spacenews.com/itu-wants-megaconstellations-to-meet-tougher-launch-milestones/?fbclid=IwAR0VpMhgrwveNmii\\_mNkC2a8inzFnG9Lhc\\_aspFLgAG\\_RoPcD4W6AsC5pII](https://spacenews.com/itu-wants-megaconstellations-to-meet-tougher-launch-milestones/?fbclid=IwAR0VpMhgrwveNmii_mNkC2a8inzFnG9Lhc_aspFLgAG_RoPcD4W6AsC5pII). Accessed July 2019
- Hertzfeld HR (2002) Technology transfer in the space sector: an international perspective. *J Technol Transf* 27(4):307–309
- HoC (2017) Space sector report. House of Commons Committee on Exiting the European Union, London

- ITU (2015) Improving the dissemination of knowledge concerning the applicable regulatory procedures for small satellites, including nanosatellites and picosatellites, Resolution ITU-R 68. ITU, Geneva
- ITU (2016) Workplan timeline process and deliverables for the future development of IMT. Unpublished Document, International Telecommunications Union, IMT-ADV/2 Working Group TECH, Meeting 24 June, ITU, Geneva
- OECD (2019) The space economy in figures: how space contributes to the global economy. OECD Publishing, Paris. <https://doi.org/10.1787/c5996201-en>
- PriceWaterhouseCoopers (2019) Main trends and challenges in the space sector. PWC, Paris
- Reagan R (1985) Determination under Section 301 of the Trade Act of 1974, memorandum for the United States trade representative. The President of the US, White House, Washington, DC
- Rostow E (1968) President's task force on communications policy, final report. Superintendent of Documents, US Government Printing Office (GPO 0-351-636), Washington, DC
- Snow M (1976) Communication via satellite – a vision in retrospect. A.W. Sijthoff International Publishing Company, Boston
- Snow M (1987a) National monopoly in INTELSAT: cost estimation and policy implications for a separate system issue. *Telematics Inform* 4(2):133–150
- Snow M (1987b) An economic issue in international telecommunications: national monopoly in commercial satellite systems. In: Macauley MM (ed) *Economics and technology in space policy*. R.F.F., Washington, DC
- USAF (2013) Global horizons final report. United States Air Force, SAF/PA Public Release case no. 2013-0434, June, US
- Zervos V (1998) Competitiveness of the European space industry, lessons from Europe's role in NATO. *J Space Policy* 14(1):39–47
- Zervos V (2002) The economics of the European space industry. DPhil thesis, University of York
- Zervos V (2011) Conflict in space. In: Braddon L, Hartley K (eds) *Handbook of the economics of conflict*. Edward Edgar Publishers, Cheltenham
- Zervos V (2018) Vasilis Zervos: “public goods, club goods and specialization in evolving collaborative entities”. In: Vliamos S, Zouboulakis M (eds) *Institutionalist perspectives on development – a multidisciplinary approach*. Palgrave Macmillan, Cham
- Zervos V, Siegel D (2008) Technology, security and policy implications of future transatlantic partnerships in space: lessons from Galileo. *Res Policy* 37:1630–1642



# Views on Space Security in the United Nations

# 76

Massimo Pellegrino

## Contents

Introduction .....	1536
Defining Space Security .....	1537
Space Security in the UN System .....	1538
Space Security Within UN International Security and Disarmament Settings .....	1541
1980s and 1990s: PAROS and the Search for Various Space CBMs .....	1542
2000–2015: Draft PPWT and New GGE on TCBMs – Parallel Efforts on Legally and Non-Legally Binding Instruments .....	1543
2015–2016: Toward a Joined-Up Approach to Space Security .....	1546
2017–Today: New GGE on PAROS, CD Subsidiary Body 3, and UNDC WG on TCBMs – Three Parallel Initiatives for Short- and Long-Term Solutions .....	1546
Space Security Within UN Space Settings .....	1549
The United Nations Committee on the Peaceful Uses of Outer Space .....	1550
The UN COPUOS Working Group on the Long-Term Sustainability of Outer Space Activities .....	1551
The United Nations Office for Outer Space Affairs .....	1554
Conclusions .....	1554
References .....	1556

## Abstract

As a forum for discussing international approaches to global challenges, the United Nations (UN) attaches great importance to space security. While no single venue addresses all aspects of space security, multiple UN bodies have become essential multilateral fora for discussing these issues. Against this backdrop, this chapter offers a definition of space security that reflects the different connotations with which this term is used within various UN entities. It then reviews and analyzes the role that relevant UN bodies and fora play in

---

M. Pellegrino (✉)  
Vienna, Austria  
e-mail: [massimo.pellegrino@community.isunet.edu](mailto:massimo.pellegrino@community.isunet.edu)

the international discourse on space security, with particular regard to the work being made within both international security (UNGA 1st Committee, CD, UNDC, UNODA, UNIDIR) and space (UNGA 4th Committee, COPUOS, UNOOSA) settings of the UN. The chapter concludes that the diverse initiatives discussed within the different UN entities indicate the increasing pressures facing the international community in addressing all aspects of space security; that substantial differences still exist among states over priorities, methodologies, mechanisms, and settings to tackle key space security challenges; and that the existence of political will that accommodates, rather than eliminates, these differences can prove effective in finding common ground for shared action.

---

## Introduction

The concept of space security features prominently in current discussions and debates pertaining to both international security and disarmament, as well as peaceful uses of outer space. It has become a widely used concept, often without a common understanding. While efforts abound, little success has been achieved in developing an accurate, commonly accepted definition of space security or a consensus understanding of the concept that provides a meaningful framework for evaluating what it encompasses, which factors contribute to and detract from it, or agreed upon metrics to measure it (a positive exception is the Space Security Index project, <http://spacesecurityindex.org>). There is even a lack of clarity on its constituent elements: not only is there as yet no universally accepted definition of outer space under international or domestic law, but the terms security, safety, and sustainability (and stability and predictability, too) are also often used interchangeably, partly because their boundaries are blurring (Box 1).

### **Box 1: Etymology and Strict Meaning of Space Security, Safety, and Sustainability**

#### **Space Security**

Security derives from Latin *securitas -atis* (noun) or *secūrus* (adjective), composed of the privative *se-* “without” and *curā* “care” (but also “worry,” “anxiety,” “preoccupation,” “concern,” and so “threat”) or *caveo* “to pay attention to,” similar to Latin *sine cūrā* “without care, carefree” which led to English sinecure. The condition of “security” is about being free of threats (i.e., deliberate hostile actions). Strictly speaking, space security describes a state of affairs in which space systems are free of threats.

#### **Space Safety**

Safety derives from Latin *salūs -ūtis* (noun) or *salvus* (adjective), which literally means health and well-being (noun) or healthy, unhurt, and unharmed

(continued)

**Box 1:** (continued)

(adjective). The condition of “safety” is about not being harmed. Space safety describes a state of affairs in which space systems are sufficiently protected from, or not exposed to, manmade and natural hazards (i.e., unintentional actions). The difference between being protected from hazards and being free of threat is not always easily seen.

**Space Sustainability**

Sustainability derives from Latin *sustinēre* (verb), composed of *sus-*, variant of *sub-* “underneath,” and *tenēre* “hold,” with the meaning of “to hold up,” i.e., preventing a system from collapsing. Sustainability is a concept that is generally being understood as the ability of carrying out a certain activity in the present while safeguarding the surrounding environment for the future, with particular regard to the resources therein contained, which are scarce, limited, and not always renewable. Space sustainability thus refers to a situation in which outer space will continue to be accessible to future generations on an equitable basis and its resources still available for meeting societal needs.

The rapid pace of change in both the space and security domains risks making a definition obsolete or outdated. This problem is also compounded by the different interpretations (not always publicly available) that space actors, especially space-faring nations, attach to space security. For some actors, it is primarily linked to the potential for space weaponization and an arms race in outer space, while for other actors, space security is being concerned with the development of direct-ascent or co-orbital antisatellite (ASAT) and other counterspace capabilities (e.g., kinetic or directed energy weapons, electronic and cyber warfare, etc.); contested space operations; creation and proliferation of space debris (which also poses dangers for destructive collisions); increased congestion of (strategic) orbits; uncontrolled satellite reentries; competition for and saturation of limited natural resources such as orbital slots and radio-frequency spectrum; unintentional radio-frequency interference; the proliferation of new space technologies and dual-use capabilities (e.g., active debris removal and on-orbit satellite servicing above all); or space weather phenomena.

Achieving a mutual understanding of the different facets of space security can thus be difficult, but it is a prerequisite not only to understand how space security issues are dealt with and addressed in the most important multilateral forum for states – the United Nations (UN) – but also to develop common approaches and responses to this global challenge.

**Defining Space Security**

Space security is a complex term that can have several meanings dependent upon the context of its usage. Attempts to precisely define it are relatively recent and

need to be contextualized (► [Chap. 2, “Definition and Status of Space Security”](#); Sheehan 2015). Regardless of how one defines outer space, space security can generally be understood as being concerned with the absence of any threats to space assets. It refers to a state of affairs in which space actors are free from third party’s actions and interferences preventing them from effectively accessing and using outer space. This preliminary definition is based on a general understanding of the term security applied to outer space and does not specifically take into account how the politics of space security have morphed since the beginning of the space race.

During much of the Cold War, security had a very specific connotation, since it was referred to military threats that could undermine the very existence of a state, notably nuclear strikes, conventional armed forces of adversaries, or even internal uprisings to overturn the *status quo*. Space security was primarily addressed through a military lens, in terms of both the contribution of military satellites for security purposes on earth (e.g., the maintenance of strategic stability above all) and the military threats to space systems and the risks associated with certain uses of outer space (e.g., earth-to-space and air-to-space missiles, explosive kinetic co-orbital systems, high-altitude and low outer space nuclear explosions).

Today’s space and security realities have morphed however. Security threats go beyond purely military ones and embrace several aspects. Similarly, the number of players interested in space capabilities has grown. Satellites serve a wider audience than the military and are used for an ever-increasing range of non-security applications providing a wealth of socioeconomic benefits.

This expansion in space activities has resulted in a heightened focus on security and has led to new conceptions of space security that focus not only on military matters but also on how to reduce risks of any kind to the space infrastructure and ensure that space operations can be safe, secure, and sustainable in the long term (Pellegrino and Stang 2016). There is thus an alignment of interests between the space and security communities (and the general public, too) to pursue a wider space security discourse for preserving the sustainability and stability of the space environment, while ensuring protection and freedom from hazards and threats to the effective access to, and use of, outer space (Pellegrino et al. 2016). While military space actors will continue to influence the international discourse on space security, for those actors without major military reliance on space, space security is primarily related to the absence of any risks and dangers to space systems and the maintenance of outer space as stable and sustainable environment. The premise is that not only does space security concern traditional and emerging space actors but also a plethora of individuals who benefit from the services enabled by space-based capabilities.

---

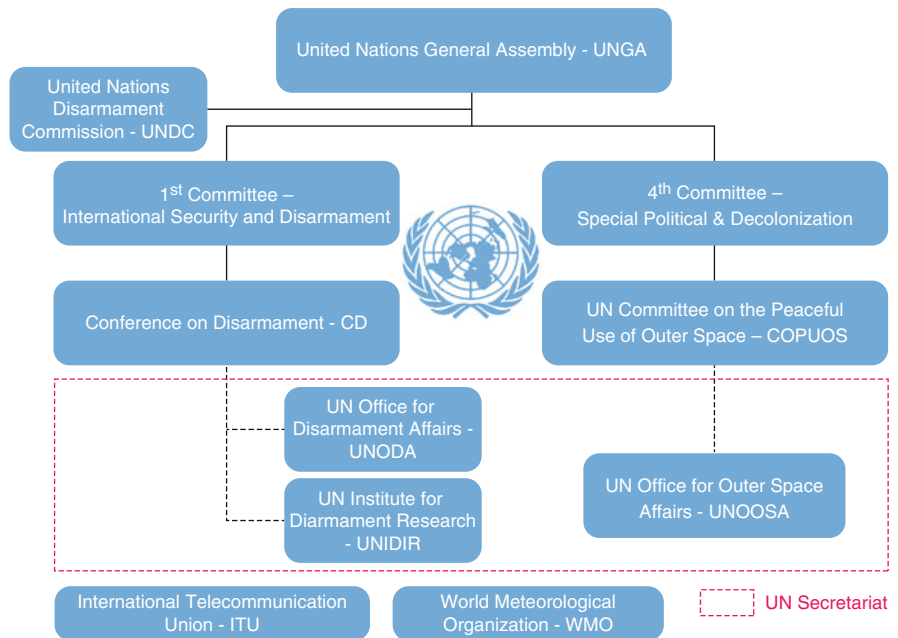
## Space Security in the UN System

The UN remains the primary multilateral forum to discuss and pursue initiatives on space security. While, as of today, there is no single venue for addressing all aspects of space security, multiple UN bodies have become essential multilateral fora

for discussing these issues, each with their own specific mandate and remit (Fig. 1). These entities are spread between New York (United States), Geneva (Switzerland), and Vienna (Austria) and include the following:

- United Nations General Assembly (UNGA), particularly its First Committee (Disarmament and International Security) and Fourth Committee (Special Political and Decolonization) in New York.
- United Nations Disarmament Commission (UNDC) in New York.
- Conference on Disarmament (CD) in Geneva.
- United Nations Office for Disarmament Affairs (UNODA) in Geneva and New York.
- United Nations Institute for Disarmament Research (UNIDIR) in Geneva.
- United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS) in Vienna.
- United Nations Office for Outer Space Affairs (UNOOSA) in Vienna.

The First Committee of the UNGA, which meets annually in October, is responsible for international security and disarmament matters and is where the Conference on Disarmament reports on its work, including on space security issues. The CD is the single multilateral disarmament negotiating forum of the international



**Fig. 1** Main UN bodies involved in space security

community and is supported by UNODA, which serves as its secretariat and provides support for norm-setting in the area of disarmament. The UNDC is an open-ended deliberative body and subsidiary organ of the UNGA and provides guidelines and recommendations on various disarmament-related issues, including space security. The UNIDIR is the UN's in-house think tank providing independent analysis and research on a wide range of international security issues and is well known for its annual space security conference providing a 1.5-track forum for dialogue on the policy and politics of outer space security at the multilateral level.

The Fourth Committee of the UNGA, which meets annually in November, deals with special political and decolonization issues, including outer space, and is where the UN Committee on the Peaceful Uses of Outer Space reports on its work. The UN COPUOS is the primary international forum for the development of rules and laws governing activities in outer space. It has a purely civilian focus and does not work on military or weaponization issues. Its work is supported by UNOOSA, which serves as its secretariat and promotes international cooperation in the peaceful use and exploration of space and in the utilization of space science and technology for sustainable economic and social development.

In addition to this, within the UN system, the International Telecommunication Union (ITU) and the World Meteorological Organization (WMO) are involved, too, in space security-related issues. The ITU allocates global radio-frequency spectrum and satellite orbital slots and addresses harmful radio-frequency interference. The WMO has been coordinating international efforts for space weather activities – an area of growing importance for the security community since space weather affects the continuous availability of critical space systems. Under the umbrella of the UN, the International Committee on Global Navigation Satellite Systems (ICG) has been working since 2006 to facilitate compatibility, interoperability, and transparency between all of the satellite navigation systems, including on aspects such as GNSS spectrum protection and interference detection and mitigation.

Representatives from these and other UN entities meet every year at the United Nations Inter-Agency Meeting on Outer Space Activities (UN-Space) to enhance coordination of space-related activities within the United Nations system, including on space security issues. An example of deliverable within this framework includes the UN-Space special report on the implementation of the report of the Group of Governmental Experts on Transparency and Confidence-Building Measures in Outer Space Activities (A/AC.105/1116), which was submitted to COPUOS in June 2016.

Multilateral discussions on space security take place in all of these venues which, for argument's sake, can be classified into two main categories: international security and disarmament settings and space settings. The former include the UNGA First Committee, UN Disarmament Commission, Conference on Disarmament, UN Office for Disarmament Affairs, and UN Institute for Disarmament Research; the latter include the UNGA Fourth Committee, UN Committee on the Peaceful Uses of Outer Space, and UN Office for Outer Space Affairs. The following chapters examine how space security issues are dealt with in these settings, what role each UN body plays in the international discourse on space security, which perspectives of



space security are prioritized therein, and which initiatives and approaches are underway to address space security issues.

---

## **Space Security Within UN International Security and Disarmament Settings**

The consideration of space security from a non-proliferation, arms control, and disarmament perspective has a long record. Attempts to protect the outer space environment and prevent indiscriminate harm to satellite systems, including one's own, have existed since the late 1950s, when the Soviet Union and the United States were engaged in negotiations on a nuclear test ban and refrained from the further testing of nuclear weapons in outer space as they recognized the incompatibility of such tests with both human spaceflights and military uses of satellites (Moltz 2014, p. 29). These discussions produced formal agreements prohibiting both nuclear tests and explosions in outer space (Article I of the Partial/Limited Test-Ban Treaty, 1963), as well as the placement and stationing of weapons of mass destruction (WMDs) in outer space or on celestial bodies (Article IV of the Outer Space Treaty, 1967).

In the decades since then, there have been multiple attempts to agree on additional norms and rules for the secure use of space, including through extending the Outer Space Treaty's ban on WMDs in outer space to weapons of any kind. These multilateral efforts have primarily included draft treaties for arms control, Transparency and Confidence-Building Measures (TCBMs), and (annual) UNGA resolutions, as well as talks in the Conference on Disarmament and in the UNGA and its First Committee under the agenda item entitled "Prevention of an Arms Race in Outer Space," commonly referred to as PAROS.

From the first discussions until today, there has been a permanent split between Soviet/Russian- and Chinese-led efforts toward a legal instrument that prohibits the placement and deployment of weapons in outer space and the views of most Western states according to which proposals for arms control measures would need to be comprehensive and precise and have proper mechanisms of monitoring, verification, and compliance (Pellegrino 2017, p. 9).

PAROS discussions and related proposals have thus become bogged down over incompatible national priorities. While the United States, for example, has an interest in defending its own freedom of action in, through, and from outer space – especially in the event that it becomes an actual war-fighting domain – China and Russia have long been concerned about the potential for space-based missile defense systems, which could undermine strategic stability and their nuclear deterrence capabilities (Hitchens 2015, p. 509).

However, the need for a re-energized dialogue on space security and the urgency of making progress, at least on those areas where there seems to be consensus, have encouraged the international community to find alternatives for moving forward, in terms of both fora in which to pursue space security dialogues and approaches for short- (e.g., non-legally binding, voluntary measures) and long-term (e.g., legally binding instruments) solutions.

The next sections review and analyze the efforts that have been made since the early 1980s within UN international security and disarmament settings to advance space security, favoring an approach based on functionality rather than a fixation on forum.

## **1980s and 1990s: PAROS and the Search for Various Space CBMs**

Space security as an arms control and disarmament topic has a long history at the United Nations (Meyer 2011). Specific initiatives on PAROS have been discussed at the UN since August 1981, when the Soviet Union requested the Secretary-General to include the issue of space weaponization as a supplementary item in the agenda of the UN General Assembly (A/36/192). At its 36th session in December 1981, the UNGA passed two PAROS resolutions, namely, A/RES/36/97C by the Western Europe and Others Group (WEOG) and A/RES/36/99 by the Eastern European and other states. While both resolutions recognized the urgency to negotiate in the Conference on Disarmament a multilateral international agreement on PAROS, there was a substantial difference in the focus of the proposed agreements, which shows the divergence of interests and threat perceptions that has accompanied space security discussions until today. While the first resolution requested the CD to consider negotiations of an agreement to prohibit antisatellite systems, the second resolution requested the CD to start negotiating a treaty to ban the stationing of weapons of any kind in outer space.

The issue was then referred to the Conference on Disarmament. In 1982, PAROS was added as an item of the CD agenda. In 1985, after a few years of consultations, an Ad Hoc Committee of the CD on PAROS was established. Already from the first discussions in the Ad Hoc Committee, there was a rift between those states belonging to the Group of 21 and Eastern states which wanted to start negotiations on PAROS and the Western states which wanted substantive consultative work before moving to actual negotiations. Another issue for disagreement became the focus of the work of the Ad Hoc Committee. The majority of states noted that the existing legal framework governing the use of space could not prevent the risk of an arms race in outer space and should therefore be amended, while Western states were reluctant to regulate space activities further and encouraged wider compliance with existing international agreements.

With limited progress on PAROS and on negotiating new legal instruments, attention was placed on non-legally binding, voluntary measures that focus more on the degree of care with which space activities are conducted and communicated, than on which kind of orbital systems are actually deployed in outer space (Pellegrino et al. 2016). As a result, various forms of Transparency and Confidence-Building Measures (TCBMs) for outer space activities were discussed both at the CD and UNGA.

In the CD, discussions on Confidence-Building Measures (CBMs) took place in the framework of the above-mentioned Ad Hoc Committee on PAROS and focused on the transparency of pre-launch activities, rules of the road, and other measures

required for monitoring purposes. In parallel, at its 45th session in December 1990, the UN General Assembly passed resolution 45/55B, requesting the Secretary-General to appoint a Group of Governmental Experts (GGE) to carry out a study on the application of CBMs in outer space. The group was made up of 10 representatives and convened four times in New York between July 1991 and July 1993. The consensus final report (A/48/305), on which some reservations were made by the US government, was submitted to the Secretary-General for transmission to the General Assembly at its 48th session in October 1993.

However, even without the pressures and expectations of legally binding arms control agreements, some divergence of views remained between those who wanted CBMs to be a stepping-stone toward legally binding treaties and those who considered them to be a valid alternative. Thus, neither did proper follow-up ensue from the work of the first GGE, nor relevant progress was made in the Ad Hoc Committee of the CD (CD/1271). Even more worrisome, the mandate of the Ad Hoc Committee on PAROS was not renewed after 10 years of work and ended in August 1994. Despite the adoption of annual UNGA resolutions on both PAROS and TCBMs and the efforts to re-establish the Ad Hoc Committee, no substantial discussions on space security cooperation took place in the late '90 and progress was prevented even due to the CD's inability to agree and implement a program of work.

### **2000–2015: Draft PPWT and New GGE on TCBMs – Parallel Efforts on Legally and Non-Legally Binding Instruments**

With the potential for a renewal of the mandate of the Ad Hoc Committee being slim, new stimulus for discussion was offered by China and Russia. In February 2000, China submitted to the CD a Working Paper (CD/1606) on PAROS outlining, inter alia, basic elements for a new international legal instrument prohibiting the testing, deployment, and use of weapons, weapon systems, and components in outer space. In June 2002, China and Russia joined forces and submitted to the CD a joint Working Paper (CD/1679) on PAROS, outlining possible elements for a future international legal agreement to prevent the deployment of weapons in outer space as well as other threats to outer space objects.

The United Nations Institute for Disarmament Research also played an important role in facilitating dialogue through track 1.5 diplomacy and identifying potential avenues for the future. In particular, since 2002, UNIDIR has supported multilateral space security diplomacy via their annual space security conference, the report of which was for many years submitted by Canada as an official CD document.

However, it was only toward the end of the decade that new impetus was given. On 12 February 2008, after 6 years of discussions (see UN Documents CD/1769 and CD/1818), China partnered again with Russia in proposing to the CD a new PAROS legal instrument (CD/1839), namely, a draft treaty on the "Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force against Outer Space

Objects” (PPWT), an updated text of which (CD/1985) was submitted on 10 June 2014. Its declared aim is to fulfill the principle of peaceful use of outer space, extending the Outer Space Treaty’s ban on WMDs in outer space to all weapons. In particular, the draft PPWT calls on adhering states not to place any weapons in outer space and not to resort to the threat or use of force against outer space objects, including through terrestrially-based weapons (Pellegrino 2017, p. 20). At present, the draft treaty does not propose any verification regime for effective monitoring and compliance, but it contains some elements for verification and resolving grievances in the form of consultative mechanisms. Critics of the PPWT, however, have noted that the proposal still suffers from a number of flaws (Pellegrino et al. 2016; see also UN Document CD/1998). For example, it ignores threats to space systems from debris-generating ASAT tests and issues related to dual-use technologies. And while prohibiting the deployment of any weapons in outer space, the proposed PPWT allows their development, production, possession, testing, use, and storage. Importantly, there are some definitional issues that need to be further addressed – the term “weapon in outer space,” for example, is still an issue for disagreement given the dual-use nature of many space technologies. In its current form, the PPWT has thus been seen as a near useless arms control treaty (Pellegrino and Stang 2016). Doubts about the PPWT that have contributed to slowing international acceptance in the CD also derive from the fact that, while advancing PAROS initiatives, the proponents of the treaty are believed to develop and deploy counterspace capabilities, as well as to practice maneuvers and proximity operations that have been perceived as weapons tests (Rajeswari Pillai Rajagopalan 2017).

With limited progress on any new treaty, greater emphasis was placed once again on non-legally binding, voluntary measures. They consist of both guidelines and “rules of the road” for how to safely conduct space operations and TCBMs for how to communicate about space activities in order to enhance trust among space actors. Following discussions instigated by Russia and tabled in the UNGA’s First Committee since 2005 (A/RES/60/66), in December 2010 the UNGA adopted resolution 65/68 calling for the creation of an expert group to study outer space TCBMs. The following year, Secretary-General Ban Ki-moon established the Group of Governmental Experts (GGE) on Transparency and Confidence-Building Measures in Outer Space Activities to investigate ways to improve international cooperation and reduce the risks of misunderstanding and miscalculations in outer space activities. The GGE, with representatives from 15 countries under the chairmanship of the Russian Federation, presented its Report (A/68/189) in July 2013 with recommendations for states and international organizations to implement on a voluntary basis two main types of TCBMs. The first includes information exchange on space policies and programs, space military expenditures, and registrations and orbital parameters of space objects. The second includes notifications related to outer space activities, such as launches, maneuvers, reentries, malfunctions, breakups, and emergencies. The Report also encourages states to open their space launch sites and facilities to visits, create consultative mechanisms to ensure continued dialogue, and pursue cooperation and outreach activities,

including with new and non-space powers. The GGE Report and its recommendations were universally welcomed by the international space and security communities. In particular, the work of the GGE was seen by many states as a pragmatic step forward and as a model for how to quickly and effectively produce a consensus report. However, implementation of the Report's recommendations has been slow, especially by those parties which had expressed diplomatic support. A major focus going forward is how to effectively ensure compliance with the identified set of TCBMs and other recommendations contained therewith, an aspects that has more recently been jointly addressed by UNOOSA and UNODA (Pellegrino 2017).

While the GGE noted the work made in UN and non-UN fora to advance space security cooperation, the existing commitments related to non-proliferation and disarmament, and the introduction by several states of policies of not being the first state to place weapons in outer space, the Report and its recommendations do not specifically cover any issues relating to arms control in space. However, the continuing appeal of such arms control rhetoric, and a widespread concern about the potential for space weaponization, found some success in the UN and contributed to buttressing anti-Western sentiment.

Since 2014, the Russian initiative (A/RES/69/32) on “No First Placement of Weapons in Outer Space” (NFP) has indeed passed with only a few states in opposition and enjoys formal support by about 45 states as sponsors or cosponsors. The rationale behind this resolution is to establish the conditions to maintain outer space as a peaceful environment by asking states to refrain from being the first to deploy weapons in space. Its declared value lies in its politically binding nature, as it can be regarded as a TCBM that increases the level of predictability in outer space activities without needs for verification. This initiative has some similarities with the PPWT and other efforts in the CD under the PAROS agenda item. Doubts about the viability of the NFP as a measure to genuinely contribute to space security have thus been raised. For example, in addition to definitional issues about what constitutes a weapon in outer space, critics point out that the NFP initiative does not fulfill the criteria for TCBMs as developed by the GGE's consensus Report and that it may entice states to preemptively develop offensive space capabilities and place them in space once a party first breaks the agreement. Deprived of the adjective “first” – which seems to legitimize the weaponization of outer space in the event that a state introduces weapons in outer space – the NFP initiative may encounter different (and more positive) reactions. Nonetheless, the voting split in the General Assembly is worth noting when considering how the international community sees space security moving forward (during the period 2014–2018, the number of states in favor of the NFP ranged from 126 to 131, those abstaining from 40 to 48, and those in opposition from 4 to 12). These diplomatic differences are problematic and remain a critical factor in shaping the international politics and policies on the security of outer space, potentially affecting efforts to push forward and win support for other space security initiatives (Pellegrino 2017).

## **2015–2016: Toward a Joined-Up Approach to Space Security**

The work of the 2013 GGE marked an important milestone in the context of space security cooperation, especially at the United Nations level. The GGE Report of July 2013 recommended that coordination be established between the Office for Disarmament Affairs, the Office for Outer Space Affairs, and other appropriate United Nations entities, breaking the silos that for many years had permeated the UN approach to space security. This coordination took the format of both joint ad hoc meetings of the UNGA First and Fourth Committees, as well as closer cooperation between UNODA and UNOSA, including in the framework of the UN-Space, and occasionally UNIDIR.

On 22 October 2015, the First and Fourth Committees of the UN General Assembly held a joint ad hoc meeting calling for a holistic and synergistic approach to address challenges to outer space security and sustainability. Two years later, on 12 October 2017, following adoption of resolution 71/90 of 22 December 2016, the First and Fourth Committees convened a second joint panel discussion as a contribution to the fiftieth anniversary of the Outer Space Treaty. Differently from the first meeting, this panel discussion saw a number of interventions from non-UN and non-MS representatives and brought some fresh views on the multi-faceted aspects of space security, including on commercial space and emerging technology threats to space activities (UNOOSA 2017).

While these meetings contributed to making the debate larger and reiterated the need for better overall coordination on the safety, security, and sustainability of outer space activities, they also accentuated the already extant divergences between those wishing to prioritize legally binding arms control agreements and those believing that non-discriminatory TCBMs and other conduct guidelines could provide a pragmatic way forward.

Closer cooperation between other appropriate UN entities took place, too. In particular, UNOOSA and UNODA, with contribution from UNIDIR, ITU, and WMO, prepared the UN-Space special report (A/AC.105/1116) on the role of United Nations entities in supporting member states in the implementation of outer space TCBMs, which was submitted to the COPUOS in June 2016. Another positive step in this direction was the 10th UN Workshop on Space Law held in September 2016, which saw UNOSA, UNODA, and UNIDIR partnering again (with the support of the Secure World Foundation) to discuss the contribution of space policy and law to space governance and space security.

## **2017–Today: New GGE on PAROS, CD Subsidiary Body 3, and UNDC WG on TCBMs – Three Parallel Initiatives for Short- and Long-Term Solutions**

Although there is no evidence of a full-scale development and deployment of weapons to project force in, through, or from outer space, the latest technological developments in counterspace capabilities (Weeden and Samson 2019) orientations

in military doctrines (United States Department of Defense 2019), and the continuing appeal by some states of outer space as a warfighting domain may suggest that some types of weapons can already be deployed in outer space for use in conflict. This has raised concerns in recent years over the prospect of an impending arms race in outer space and reinvigorated discussions on space security matters. The year 2017 represented an important cornerstone for the future of space security diplomacy, as states seemed to have found new source of political will to move forward.

In February 2017, the UN Secretary-General issued a report (A/72/65) prepared by UNODA on TCBMs in outer space activities, reproducing the substantive text of the special report by UN-Space (A/AC.105/1116) and incorporating updates and views received from the contributing entities and some states.

In its 2017 session from 3 to 21 April 2017, the United Nations Disarmament Commission held informal discussions on the practical implementation of outer space TCBMs with a view to taking up the issue in its 2018–2020 three-year cycle.

In February 2017, under decision CD/2090, the Conference on Disarmament established a Working Group on the “way ahead” to identify common ground for a program of work with a negotiating mandate. From 14 to 16 June 2017, the Working Group convened to address the prevention of an arms race in outer space (agenda item 3), with discussions featuring the linkages between space security and strategic stability, instruments of soft law, and legally binding instruments. Ambassador Htin Lynn of Myanmar chaired the meetings, with Ambassador Hellmut Lagos Koller of Chile co-facilitating them in his capacity as friend of the chair. While these discussions did not reconcile the divergent views of states concerning the nature of space threats and the most appropriate ways of responding to them, there was widespread agreement on the urgency of adopting immediately applicable measures. In particular, it was noted that space technology is inherently dual-use and can contribute to both maintaining and disrupting strategic stability; that, while the potential for space weaponization is a major concern, there are other dangers to space systems, such as ground-based kinetic weapons, directed energy weapons, means of electronic warfare, space debris, and space weather; that the current legal regime governing the use of space is in need of some updating and that instruments of soft law are useful supplements to legally binding provisions; that avoiding indiscriminate harm in outer space, such as that resulting from destructive ASAT tests, and prohibiting intentional creation of space debris might be an avenue for the future and form the basis for future consensus; and that there are a number of actions in space that can be perceived as hostile for which TCBMs and norms of behavior can have measurable impacts and be a faster step to move forward.

All of this work gave new impetus to space security discussions and was instrumental in laying the foundation for more substantive work, both on voluntary measures and legally binding instruments. In particular, in 2018, three separate initiatives were launched in parallel within the UN system, each with a different timeframe.

First, on 24 December 2017, the UNGA adopted resolution 72/250 establishing a new Group of Governmental Experts (GGE) on Further Practical Measures for the Prevention of an Arms Race in Outer Space. The mandate of this GGE was to

explore substantial elements of a possible legally binding instrument, including on the prevention of the placement of weapons in outer space, using the draft PPWT as a very minimum basis for discussion. Ambassador Guilherme de Aguiar Patriota, Permanent Representative of Brazil to the CD, was named the chair of the GGE, with UNIDIR acting as the technical expert. The GGE, with a membership of up to 25 representatives, met for two two-week sessions in Geneva, one from 6 to 17 August 2018 and the other one from 18 to 29 March 2019. A two-day open-ended intersessional informal consultative meeting was also held in New York on 31 January and 1 February 2019 to allow member states and the broader space community to engage in further discussions and to comment on an interim report by the chair on the work of the GGE (Patriota 2019). At its final session in March 2019, the GGE could not reach consensus on a final report. Nonetheless, discussions within the GGE have been if nothing else instrumental in identifying the pros and cons of new legal instruments and in offering a platform to discuss highly debated issues, such as definitions and verification (Meyer 2018).

Second, on 19 February 2018, through decision CD/2119, the Conference on Disarmament agreed to establish five subsidiary bodies to address individual agenda items in the absence of an overall program of work. Subsidiary Body 3 was tasked with focusing on the Prevention of an Arms Race in Outer Space. Ambassador Guilherme de Aguiar Patriota was appointed coordinator, with UNIDIR acting as the technical expert. Over the course of 2018, this Subsidiary Body met seven times and agreed on a consensus report which was submitted to and adopted by the CD plenary. This report, labeled as CD/WP.611, reviews the existing normative and institutional framework, identifies threats that raise major concerns among member states, and puts forward possible solutions, including the recourse to other UN fora to move discussions forward. Unfortunately, due to political difficulties, the CD was unable to adopt the report of Subsidiary Body 4 and therefore the final report to be sent to the UNGA. However, the CD was able to agree on and adopt a procedural report, which includes as appendixes all official documents of the Conference on Disarmament, summary records, process verbal, and reports of subsidiary bodies.

Third, at its organizational meeting on 21 February 2018, the United Nations Disarmament Commission agreed to include space security in its work program for the 2018–2020 cycle and to establish a Working Group to promote the practical implementation of outer space TCBMs with the goal of preventing an arms race in outer space. In particular, this Working Group is tasked with looking at how the recommendations contained in the consensus report of the 2013 GGE can be implemented and made operational, in an attempt to re-energize discussions over what was seen as a model for effective space security diplomacy. The UNDC Working Group held several meetings during its two-week sessions in April 2018 and April 2019, with a last meetings session being anticipated in April 2020, when it is expected to make some recommendations to give substantive effect to the 2013 GGE Report. However, even though the Working Group focuses on voluntary measures that are not legally binding, the consensus rule by which the UNDC operates and the limited track record of success that the UNDC has



experienced in recent years indicate that expectations would need to be managed (Meyer 2018).

While the GGE on Further Practical Measures for PAROS and the Conference on Disarmament failed to achieve consensus on a final report and on a decision that would have re-established CD Subsidiary Body 3, respectively, all of these three separate initiatives have allowed for parallel discussions on two distinct approaches to space security – one which looks at more robust solutions through the lens of legally binding arms control agreements and the other one which looks at short-term solutions through the lens of voluntary, non-legally binding measures. By holding parallel discussions, proponents of treaties and TCBMs can still work together, potentially impacting efforts to win support for their own preferred approach.

---

## Space Security Within UN Space Settings

The consideration of space security from the perspective of peaceful uses of outer space has a long history, too. Earliest records date back to January 1958 when, in the context of Soviet-US relations for reducing international tensions, US President Eisenhower made a proposal to use outer space only for peaceful purposes and to deny it to the purposes of war (United States Department of State 1958). On 15 March 1958, a concrete proposal on the topic was submitted by the Soviet Union for consideration by the 13th session of the UN General Assembly. Through resolution 1348 (XIII) of 13 December 1958 – the first ever UN resolution related to outer space – the UNGA established an ad hoc Committee on the Peaceful Uses of Outer Space to discuss the scientific and legal aspects of the exploration and uses of outer space. Although these issues may not seem closely connected to security matters, they were very relevant. By advancing proposals on the peaceful uses of outer space, both superpowers reaffirmed the importance of stopping using space for the testing of missiles designed for military purposes. Not only was outer space seen as instrumental in increasing the power of new types of weapons to the detriment of the mankind but also, more importantly, controlling the uses of outer space implied controlling the development of missiles as carriers of weapons (Jacobson and Stein 1966).

In the decades since then, there have been multiple attempts in UN space settings to regulate the different uses of outer space, including on aspects pertaining to the broader perspective of space security. These multilateral efforts have included international agreements, treaties, and conventions; UNGA declarations and legal principles; UNGA resolutions; and guidelines and rules for safe and sustainable space operations; as well as talks in the Committee on the Peaceful Uses of Outer Space and its subcommittees primarily under the agenda item entitled “Long-Term Sustainability of Outer Space Activities,” and in the UNGA and its Fourth Committee under the agenda item entitled “international co-operation in the peaceful uses of outer space.” From the first discussions until today, space security has been seen, on the one hand, as part of the global space governance and international cooperation efforts aimed at ensuring a certain level of order and predictability in space and, on

the other hand, as part of wider sustainability and development issues aimed at ensuring a safe and sustainable conduct of space activities both in space and on Earth. This is in line with both the initiative by COPUOS on the long-term sustainability of outer space activities and the strategic reflection promoted by UNOOSA in the lead-up to UNISPACE+50 and Space 2030, where space security is considered instrumental in achieving the 2030 Agenda for Sustainable Development.

By following an approach based on forum, the next paragraphs review and analyze the efforts that have been made in recent years within UN space settings to advance space security in its broader connotation.

## **The United Nations Committee on the Peaceful Uses of Outer Space**

The Committee on the Peaceful Uses of Outer Space (COPUOS) is a permanent body of the United Nations mandated to discuss cooperative mechanisms in space activities and to develop principles governing the exploration and use of outer space. Initially established as an ad hoc committee, the UN COPUOS promotes international cooperation in the peaceful uses of outer space, encourages information sharing and the development of national space research programs, and addresses legal issues arising from the exploration of space. The Committee has a purely civilian focus and does not specifically address military activities in space, although these may be affected by its deliberations.

As of September 2019, COPUOS comprises 92 states as committee members, with over 40 intergovernmental and non-governmental organizations being granted observer status. Decisions are made by consensus and reported to the UN General Assembly for consideration and endorsement usually on the same year. The technical work of the Committee is conducted by two subcommittees, the Legal Subcommittee (LSC) and the Scientific and Technical Subcommittee (STSC), which each convene once a year and report on their work to the Committee during its annual meeting.

The work carried out in the framework of COPUOS can readily accommodate diverse aspects pertaining to space security. For instance, the five international treaties and set of legal principles governing space activities contain a number of provisions that lay down the legal foundation for space security and associated matters. Examples include the prohibition of placement of weapons of mass destruction in orbit or on celestial bodies, the liability of launching states for damages caused by space objects, the registration of space objects, the notification of space activities, the safety of spacecraft, the prevention of harmful interference with space activities, and the avoidance of harmful contamination of the space environment.

In addition to the codification of international space law, the work of the UN COPUOS in the matter of space security has been focused on the protection of space systems and on the safeguard of the space environment. Topics such as the use of nuclear power sources in space, measures for space debris mitigation and remediation, and space traffic management have all been under consideration in the Legal Subcommittee. Likewise, space debris, space weather, near-earth objects, and other

aspects closely related to the safety and sustainability of space activities have been on the agenda of the Scientific and Technical Subcommittee for many years now. In particular, along with the work of the Working Group on the Long-Term Sustainability of Outer Space Activities, the development and adoption by COPUOS of a set of voluntary guidelines for space debris mitigation represents one of the greatest successes of the Committee in recent years (UNOOSA 2010). Building on the IADC proposal on debris mitigation (A/AC.105/C.1/L.260), the UN COPUOS seven technical guidelines (A/AC.105/890) focus on how to safely conduct space activities while limiting the proliferation of space debris. Importantly, guideline 4 recommends that the intentional creation of long-lived debris be avoided, a rule that could also be seen as a commitment by states not to test destructive ASAT weapons (Hitchens 2015). These technical guidelines have contributed to increasing understanding of what constitutes acceptable activities (and behavior) in space, and their implementation through relevant national mechanisms would be a pragmatic way forward to reduce tensions, alter threat perception, and increase stability in space. Since 2014, under the agenda item on “ways and means of maintaining outer space for peaceful purposes,” the UN COPUOS has also considered the recommendations contained in the 2013 Report by the GGE on space TCBMs, with the aim of identifying those recommendations that could ensure the safety of space operations and the long-term sustainability of outer space activities.

### **The UN COPUOS Working Group on the Long-Term Sustainability of Outer Space Activities**

Conversely to sustainability on Earth, the topic of sustainability of space activities has been on the agenda of the United Nations only since 2007, not coincidentally a few months after China’s ASAT test created thousands of long-lasting pieces of debris (Brachet 2012, 2016). At the 50th session of the UN COPUOS, then-Chair Gérard Brachet submitted a Working Paper (A/AC.105/L.268) on the future role and activities of COPUOS, suggesting that the Committee address the issue of the long-term sustainability of outer space activities and that a dedicated Working Group be set up in the STSC to develop “rules of the road” for future space operations.

In line with this proposal, an ad hoc group of experts with representatives from over 20 countries was created under the impulse of France in order to develop information exchange mechanisms and consensus-based rules of behavior for a safer and more secure space environment (see UN Document A/AC.105/C.1/L.303). The expert group worked through 2008 and 2009 to develop a document (A/AC.105/C.1/2010/CRP.3), also referred to as the “Brachet Code of Conduct,” addressing a wide range of technical issues (e.g., space debris mitigation and remediation, the safety of space operations, the electromagnetic spectrum, and space weather) and putting forth a set of preliminary recommendations. While conducted informally, this work (and that of the French Delegation to COPUOS, too) led to the creation in the UN COPUOS STSC of a Working Group on the Long-Term Sustainability of Outer

Space Activities, the terms of reference of which (A/AC.105/C.1/L./307/Rev.1) were finalized the following year in June 2011.

The Working Group was tasked with preparing a consensus report containing a set of voluntary, non-legally binding best practices guidelines for implementation by all space actors to reduce risks to space activities and ensure equitable access to outer space for the benefit of all nations. In doing so, the Working Group examined the long-term sustainability of outer space activities within the wider context of sustainable development on Earth, including the contribution of space activities to the achievement of the Millennium Development Goals. In order to examine the various aspects surrounding space sustainability and prepare candidate guidelines to be then refined and agreed upon by member states at COPUOS, the Working Group relied upon four expert groups, each with a specific focus:

- Expert Group A: Sustainable space utilization supporting sustainable development on Earth.
- Expert Group B: Space debris, space operations, and tools to support collaborative space situational awareness.
- Expert Group C: Space weather.
- Expert Group D: Regulatory regimes and guidance for actors in the space arena.

Inputs from non-state actors were welcome if submitted through the relevant member states or permanent observers, both of which were also allowed to nominate non-governmental experts to the expert groups as part of their delegation (Martinez 2015). This has allowed the substantial body of knowledge and experience of the private sector and other NGOs not to be dissipated and contributed to making the guidelines relevant to all space actors and activities throughout the entire supply chain and life cycle.

The Working Group initial mandate ran until 2014, with the total number of proposed guidelines fluctuating up to 33 as inputs from expert groups, UN COPUOS member states, and WG Chair Peter Martinez were received. In June 2014, WG Chair Peter Martinez proposed to combine the 33 draft guidelines (A/AC.105/C.1/L.339) into 16 consolidated draft guidelines (A/AC.105/2014/CRP.5), to which 3 more candidate guidelines (A/AC.105/C.1/L.340) were added in October 2014.

The Committee also agreed that work should have continued in order to finalize the draft guidelines for their approval at the plenary sessions of COPUOS in 2016 and for their subsequent referral to the UNGA also in 2016. Additional 10 guidelines and alternatives were thus introduced by input from member states in 2015, and, following a process of consolidation and refinement (and compromise, too), the total number of draft guidelines was narrowed down to 29 (Martinez 2018). Since decision on the text of each guideline is reached by consensus, progress was intermittent and a first set of 12 guidelines (A/AC.105/2016/CRP.17) could be agreed upon only during the 2016 COPUOS plenary.

As the remaining guidelines were all at different stages of readiness, the mandate of the WG was extended until June 2018. In February 2018, at the 55th session

of the STSC, agreement was reached on the preamble and 9 further guidelines (A/AC.105/C.1/2018/CRP.18/Rev.1), which are now ready for states and intergovernmental organizations to consider implementing on a voluntary basis (See UN Document A/AC.105/C.1/L.366).

Although the mandate of the WG expired in June 2018, with no final report by the WG being agreed upon, work has continued on the text of the remaining draft guidelines (A/AC.105/C.1/L.367) – as well as on specific procedures for reviewing, amending, and revising the text – with a view to reaching consensus on a final report and a full compendium of agreed guidelines to be then adopted by COPUOS and referred to the UN General Assembly. To expedite this process, a number of options were put forth by member states, including through extending the mandate of the Working Group by 1 year or establishing a new permanent Working Group. At its 62th session in 2019, the Committee decided to establish, under a five-year workplan, a new Working Group on the Long-Term Sustainability of Outer Space Activities under the STSC.

The set of 21 guidelines (A/74/20, Annex II) agreed to date, which were formally adopted by COPUOS in June 2019, are classified into four major categories and address a wide range of aspects pertaining to space activities, from policy and regulatory, to operational and safety, to international cooperation and capacity building, and to scientific and technical research and development. In particular, the guidelines include specific measures to ensure the safe and sustainable use of outer space for peaceful purposes. In recognizing the difference in capacity and capabilities among space actors, space-faring nations are encouraged to support emerging space actors in the implementation of the guidelines, as well as in the development of space capabilities in a manner that avoids potential harms for all parties concerned.

While voluntary and non-binding under international law, the guidelines may lead states to establish relevant national mechanisms for facilitating their implementation and to incorporate the principles therein contained in their national legislation.

Importantly, the long-term sustainability guidelines can be viewed as enablers for the implementation of existing TCBMs or even as TCBMs themselves, possibly providing the basis for more robust initiatives.

There have also been attempts by some delegations to introduce hard security issues into the work of COPUOS, but success has been limited, since those topics are seen as the prerogative of the CD and the First Committee of the UNGA. While the persistence of not contaminating the work of COPUOS with hard security issues may be seen as a limit to the ability of the body to make progress in the area of space security, it has actually allowed the Committee to exclusively focus on his core mandate and to make some tangible progress on safety and sustainability issues. However, like all voluntary measures, the success of this initiative will eventually depend on the extent to which space actors implement the agreed upon guidelines. The hope is that the awareness and positive momentum that this multilateral consensus-based process has created may facilitate future adoption of the guidelines.

---

## The United Nations Office for Outer Space Affairs

The United Nations Office for Outer Space Affairs (UNOOSA) is the Office of the United Nations which promotes international cooperation in the peaceful uses of outer space to achieve development goals for the benefit of humankind. In addition to serving as the secretariat of the UN COPUOS, the Office is also responsible for discharging the UN Secretary-General's responsibilities and obligations under international space law, with particular regard to the implementation of the five UN space treaties, as well as information exchange and notification mechanisms.

More specifically, UNOOSA maintains the UN Register of objects launched into outer space (Article III of the Registration Convention) and disseminates information relating to outer space activities (including discovery of harmful phenomena) provided by states (Articles V and XI of the Outer Space Treaty), which are de facto treaty-based TCBMs for enhanced space security. The Office also serves as a facilitator on notifications relating to the malfunction and re-entry of nuclear-powered space objects (Principle V of the Principles Relevant to the Use of Nuclear Power Sources in Outer Space). In its resolutions 70/82 and 71/90, the UN General Assembly also encourages UNOOSA to conduct capacity-building and outreach activities associated with space security and TCBMs in outer space activities, recognizing the positive contribution that the Office can offer in these areas. Looking forward, UNOOSA could be instrumental in the implementation of a number of TCBMs, including through providing notifications on outer space activities aimed at risk reduction, disseminating pre-launch notifications, and facilitating voluntary visits to space launch sites and facilities and to demonstrations of rockets and space technologies (Keusen 2017).

Importantly, the wider strategic review promoted by UNOOSA in the lead-up to UNISPACE+50 provided an additional opportunity to address the legal regime of outer space and global space governance, information exchange on space objects and events, and space weather services, as the thematic priorities of UNISPACE+50 have shown (see UN Document A/AC.105/2016/CRP.3). In particular, interconnection exists between the above-mentioned areas and the work of the Working Group on the Long-Term Sustainability of Outer Space Activities. With the recent tendency of merging space and development issues, and in light of the adoption of the 2030 Agenda for Sustainable Development, a safe, sustainable, and secure space environment is needed to ensure the continuous and reliable operations of space systems, including those supporting the achievement of the sustainable development goals.

---

## Conclusions

The various initiatives being discussed in the different UN fora indicate the increasing pressures facing the international community in addressing all aspects of space security and strengthening the multilateral regime governing the use of space. They also reveal substantial differences among states over priorities, methodologies,

mechanisms, and settings to address and tackle space security issues. These differences include incompatible political sensibilities and perceptions of what key space security risks are, whether the potential for space weaponization, the development of counterspace capabilities, or the proliferation of space debris; differing visions for how to address major challenges, whether by means of legally binding treaties or instruments of soft law; divergent views on the most appropriate setting in which to pursue space security diplomacy, whether in UN disarmament or space settings; and different opinions on which participants to include in the discussion (and how and when to involve them), whether to start with a like-minded core group to discuss the essence or to include, to the greatest extent practicable, as many actors as possible from the beginning (Pellegrino et al. 2016). While this proliferation of initiatives offers distinct approaches that look at both short- and long-term solutions, these proposals may end up in endless discussions, being honored only with rhetoric, or even ignored altogether. More worrisome, however, may be another challenge: deadlocks in the work of one body can be transferred over other fora, limiting progress even on those aspects on which there has traditionally been consensus.

Existing frictions among different UN bodies are also a limiting factor in pushing forward a shared agenda on space security, and so too is the long-standing division between civilian and military uses of space embedded in the UN machinery (Hitchens 2015). UNIDIR, which constitutes an invaluable forum with a frank and open dialogue on the latest challenges to the security, safety, and sustainability of outer space, could be instrumental in facilitating dialogue at all levels, both within and outside the UN, as it has always more frequently convened an ever-increasing range of established and emerging actors and stakeholders in the space and security communities with a view to exploring current trends, building bridges, and identifying potential avenues for the future. Shrinking budgets and bureaucratic politics (i.e., the promotion and protection by relevant officials of their own bureau's interests in competition with those ones of other bureau) are however hampering cooperative efforts in spite of appropriate coordination mechanisms between relevant UN entities being envisaged.

There would be great value if progress being made on space safety and sustainability in COPUOS was not seen as an end in itself, but rather as an intermediate step to create more favorable political conditions to advance discussions on hard security issues in space. The long-term sustainability guidelines are the outcome of a consensus-based process which saw the participation of all the actors engaged in arms control discussions and can be seen as a stepping-stone toward more robust international agreements.

In short, while progress has been intermittent and further work is required, especially in UN international security and disarmament settings, the future for space security diplomacy looks relatively promising, at least more than it has been in previous years. Discussions for both short- and long-term solutions will likely continue to proceed in parallel. While divergent perceptions and priorities among leading space powers still exist (and will remain), the existence of political will that accommodates, rather than eliminates, these differences can prove effective in finding common ground for future action that can be acceptable for the interests of

different states. As the nature of risks to space infrastructure and services, and the available responses, are similar (although not entirely) for all space actors – whether civilian, commercial, or military – common threat perceptions may influence how states choose to cooperate and readily serve as a basis for developing common responses and finding future consensus.

---

## References

- Brachet G (2012) The origins of the “Long-term Sustainability of Outer Space Activities” initiative at UN COPUOS. *Space Policy* 28:161–165. [https://www.academia.edu/20607722/The\\_origins\\_of\\_the\\_Long\\_Term\\_Sustainability\\_of\\_Space\\_Activities\\_initiative\\_at\\_UNCOPUOS](https://www.academia.edu/20607722/The_origins_of_the_Long_Term_Sustainability_of_Space_Activities_initiative_at_UNCOPUOS). Accessed 31 Aug 2019
- Brachet G (2016) The security of space activities. Non-proliferation papers, no. 51, EU Non-Proliferation Consortium. <https://www.nonproliferation.eu/wp-content/uploads/2018/09/the-security-of-space-activities-52.pdf>. Accessed 31 Aug 2019
- Hitchens T (2015) Space security-relevant international organizations: UN, ITU, and ISO. In: Schrogl K-U (et al) (eds) *Handbook of space security: policies, applications and programs*. Springer, New York
- Jacobson H, Stein E (1966) Diplomats, scientists, and politicians: the United States and the nuclear test ban negotiations. The University of Michigan Press, Ann Arbor. [https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1014&context=michigan\\_legal\\_studies](https://repository.law.umich.edu/cgi/viewcontent.cgi?article=1014&context=michigan_legal_studies). Accessed 31 Aug 2019
- Keusen T (2017) Safety, security and sustainability of outer space activities: UNOOSA and TCBMs looking forward. Presentation at the 2017 UNIDIR space security conference, Geneva, 20–21 April 2017. <http://www.unidir.ch/files/conferences/pdfs/safety-security-and-sustainability-of-outer-space-activities-unoosa-and-tcbms-looking-forward-en-1-1244.pdf>. Accessed 31 Aug 2019
- Martinez P (2015) Space sustainability. In: Schrogl K-U (et al) (eds) *Handbook of space security: policies, applications and programs*. Springer, New York
- Martinez P (2018) First fruits of the long-term sustainability discussions in UN COPUOS. Paper presented at the 69th International Astronautical Congress (IAC), IAC-18-E3.4.1, Bremen, 1–5 Oct 2018
- Meyer P (2011) The CD and PAROS: a short history. United Nations Institute for Disarmament Research, Geneva. <http://www.unidir.org/files/publications/pdfs/the-conference-on-disarmament-and-the-prevention-of-an-arms-race-in-outer-space-370.pdf>. Accessed 31 Aug 2019
- Meyer P (2018) Diplomacy: the missing ingredient in space security. Simons papers in security and development, no. 67/2018, School for International Studies, Simon Fraser University, Vancouver. <http://summit.sfu.ca/system/files/iritems1/18290/SimonsWorkingPaper67.pdf>. Accessed 31 Aug 2019
- Moltz J (2014) *Crowded orbits: conflict and cooperation in space*. Columbia University Press, New York
- Patriota G (2019) Interim Report by the Chair of the Group of Governmental Experts on Further Practical Measures for the Prevention of an Arms Race in Outer Space. <https://s3.amazonaws.com/unoda-web/wp-content/uploads/2019/02/oral-report-chair-gge-paros-2019-01-31.pdf>. Accessed 31 August 2019
- Pellegrino M (2017) UNIDIR space security conference report 2017. United Nations Institute for Disarmament Research, Geneva. <http://unidir.org/files/publications/pdfs/unidir-space-security-2017-en-685.pdf>. Accessed 31 Aug 2019
- Pellegrino M, Stang G (2016) Space security for Europe. European Union Institute for Security Studies, Paris. [https://www.iss.europa.eu/sites/default/files/EUISSFiles/Report\\_29\\_0.pdf](https://www.iss.europa.eu/sites/default/files/EUISSFiles/Report_29_0.pdf). Accessed 31 Aug 2019
- Pellegrino M et al (2016) Security in space: challenges to international cooperation and options for moving forward. Paper presented at the 67th International Astronautical Congress (IAC), IAC-



- 16-E3,4,12,x35460, Guadalajara, 26–30 September 2016. <https://swfound.org/media/205876/manuscript-security-in-space-iac-2016.pdf>. Accessed 31 Aug 2019
- Rajagopalan RP (2017) Space security, deterrence and strategic stability. Presentation at the 2017 UNIDIR Space Security Conference, Geneva, 20–21 April 2017. <http://www.unidir.ch/files/conferences/pdfs/space-security-deterrence-and-strategic-stability-en-1-1224.pdf>. Accessed 31 Aug 2019
- Sheehan M (2015) Defining space security. In: Schrogl K-U (et al) (eds) Handbook of space security: policies, applications and programs. Springer, New York
- United States Department of Defense (2019) Missile Defense Review. The United States Department of Defense, Washington, DC. <https://media.defense.gov/2019/Jan/17/2002080666/-1/-1/1/2019-MISSILE-DEFENSE-REVIEW.PDF>. Accessed 31 August 2019
- United States Department of State (1958) The Department of State bulletin, Vol. XXXVIII (No. 970, 27 January 1958, pp. 122–127) and Vol. XXXVIII (No. 976, 10 March 1958, pp. 376–380), US Government Printing Office, Washington, DC. <https://catalog.hathitrust.org/Record/000598610>. Accessed 31 August 2019
- UNOOSA (2010) Space Debris Mitigation Guidelines of the Committee on the Peaceful Uses of Outer Space. United Nations, Vienna. [https://www.unoosa.org/pdf/publications/st\\_space\\_49E.pdf](https://www.unoosa.org/pdf/publications/st_space_49E.pdf). Accessed 31 August 2019
- UNOOSA (2017) Joint panel discussion of the First and Fourth Committees on possible challenges to space security and sustainability. [https://www.unoosa.org/documents/pdf/gajointpanel/Co-Chair\\_Summary\\_C1-C4\\_Joint\\_Panel\\_Discussion\\_Final\\_2.pdf](https://www.unoosa.org/documents/pdf/gajointpanel/Co-Chair_Summary_C1-C4_Joint_Panel_Discussion_Final_2.pdf). Accessed 31 August 2019
- Weeden B, Samson V (eds) (2019) Global counterspace capabilities: an open source assessment. The Secure World Foundation, Washington, DC. [https://swfound.org/media/206408/swf\\_global\\_counterspace\\_april2019\\_web.pdf](https://swfound.org/media/206408/swf_global_counterspace_april2019_web.pdf). Accessed 31 Aug 2019

## Further Readings

- Brachet G (2007) Collective security in space: a key factor for sustainable long-term use of space. In: Logsdon J et al (eds) Collective security in space: European perspectives. Space Policy Institute, Elliott School of International Affairs, The George Washington University, Washington, DC
- Hersch M, Steer C (eds) (2020) War and Peace in Outer Space: Ethics, Law and Policy. Oxford University Press, Oxford. (in progress)
- Rajagopalan RP (2018) Space governance. Oxford research encyclopedia of planetary science. <https://doi.org/10.1093/acrefore/9780190647926.013.107>. Accessed 31 Aug 2019



# The Role of COSPAR for Space Security and Planetary Protection

# 77

Leslie I. Tennen

## Contents

Introduction .....	1560
The Committee on Space Research .....	1561
Foundations and Development of the Planetary Protection Policy .....	1562
Initial Activities of the Diplomatic Community .....	1562
Initial Scientific Policies .....	1562
Policies of Planetary Protection .....	1562
Scientific Regulation Through Planetary Quarantine Requirements .....	1563
Planetary Protection and the Emergence of Binding International Law .....	1565
Revisions to the PQR .....	1565
The Moon Agreement and Elaboration of Legal Regulation .....	1566
Transformation of the PQR .....	1567
Current COSPAR Planetary Protection Policy .....	1567
Categorization of Target Bodies .....	1567
Categories I and II .....	1568
Category III: Flyby and Orbiter Mission to Mars, Europa, and Enceladus .....	1568
Category IV: Lander Missions to Mars, Europa, and Enceladus .....	1569
Category V Sample Return Missions .....	1569
Human Missions to Mars .....	1570
Implementation of the COSPAR PPP by Space Agencies and Authorities .....	1571
European Space Agency .....	1572
The United States .....	1572
Japan .....	1573
Russia .....	1573
Israel .....	1574
China/India/UAE .....	1574

---

L. I. Tennen (✉)

Law Offices of Sterns and Tennen, Glendale, AZ, USA

e-mail: [Ltennen@astrolaw.com](mailto:Ltennen@astrolaw.com)

Lacuna in the Planetary Protection Policy .....	1575
Expand Target Bodies in Categories III and IV .....	1575
Missions to Phobos and Deimos Can Increase the Risk of Contaminating Mars .....	1576
Challenges to Planetary Protection by Private Sector Commercial Projects .....	1577
Conclusion .....	1578
References .....	1579

---

## Abstract

The environment of the Earth can be at risk of potential contamination from extraterrestrial material brought back to this planet by robotic and human explorers. Similarly, spacecraft sent to explore celestial bodies can carry microbes that can contaminate an extraterrestrial environment. Contamination presents significant implications for space security. The Committee on Space Research (COSPAR) of the International Science Council (ISC) has maintained a Planetary Protection Policy (PPP) to address both forward and back contamination. States have implemented the COSPAR PPP as the recognized standard to comply with international treaty obligations in regard to contamination from biological matter.

---

## Introduction

How did life begin? Are we alone in the universe? These questions are among the most essential, eternal, and enduring mysteries of science. With the advent of the space age, mankind acquired new capabilities to search for alien life. We have the technology to venture to distant worlds, conduct experiments in the pursuit of evidence of life, and even bring samples from celestial bodies back to our home planet. However, extraterrestrial matter brought back to the Earth could potentially harbor deleterious material that could jeopardize the safety and security of the entire globe. This issue of “back contamination” is not confined to the realm of science fiction but has been a significant concern since the days of the Apollo program.

Just as the environment of the Earth is in need of protection from potential harmful contamination from extraterrestrial sources, so it is also necessary to protect celestial environments from harmful contamination from terrestrial matter. The discovery of evidence of life on another celestial body would forever change humanity’s view of mankind’s place in the cosmos. The significance of such a discovery cannot be overstated, nor can it be completely comprehended in advance; therefore it is of the utmost importance that the scientific integrity of such a discovery be assured. Forward contamination of a celestial environment from terrestrial biological materials could jeopardize the scientific integrity of subsequent investigation and also could harmfully interfere with future exploration and experimentation. This directly impacts the risk of conflict between nations and threatens the safeguarding of space for peaceful endeavors.

In its most basic terms, forward contamination controls seek to ensure that any evidence of life found on a celestial body is indigenous and not of terrestrial origin. Similarly, back contamination requirements are a way to answer the question of how will we know that extraterrestrial matter brought back to the Earth will not be dangerous. The policy of planetary protection can be summarized as follows:

The conduct of scientific investigations of possible extraterrestrial life forms, precursors, and remnants must not be jeopardized.

The Earth must be protected from the potential hazard posed by extraterrestrial matter carried by a spacecraft returning from a celestial body. (Coustenis et al. 2019)

---

## The Committee on Space Research

The international diplomatic and scientific communities have acted to prevent both forward and back contamination. The United Nations has been the leading organization for the development of legal principles to protect celestial environments. The Committee on Space Research (COSPAR) has been the preeminent scientific forum for the articulation of specific policies and guidelines for planetary protection (the Planetary Protection Policy or PPP).

COSPAR was formed in 1958 by the International Council of Scientific Unions (ICSU), now the International Science Council (ISC). The membership of COSPAR is comprised of national scientific institutions and international scientific unions. The organizational structure consists of eight commissions which represent every scientific discipline involved in space research. In addition, there are ten panels which are designed to deal with issues of interest to specific segments of the space research community. The prevention of forward and back contamination is the charge of the Panel on Planetary Protection (PP Panel).

The PP Panel is appointed by the COSPAR Bureau and is led by a chair and two vice-chairs, one of which is reserved for a representative of the United Nations Office for Outer Space Affairs (UNOOSA). There is an equal number of representatives from national or international authorities and representatives from COSPAR Scientific Commission B, Space Studies of the Earth-Moon System, Planets, and Small Bodies of the Solar System, and Commission F, Life Sciences as Related to Space.

The competence of the COSPAR PP Panel is limited to forward and back contamination from biological sources. As such, it is primarily concerned with microbes and other potential organic contaminants. The COSPAR PP Panel does not otherwise consider protecting celestial bodies, unique environments, or historical sites. Nor does the COSPAR Planetary Protection Policy apply to protecting the Earth from man-made space debris or defending the planet from the impact of large asteroids or comets.

## Foundations and Development of the Planetary Protection Policy

### Initial Activities of the Diplomatic Community

In 1957, the United Nations General Assembly took the first formal steps to regulate mankind's movement into the cosmos by the creation of the *Ad Hoc* Committee on the Peaceful Uses of Outer Space (COPUOS), which became a permanent committee the following year. COPUOS conducts its work through two subcommittees, one of which is devoted to scientific and technical matters, while the other considers legal issues. Membership in the Committee has expanded over the years to include all states actively launching and performing missions in space. Currently 95 nations are members of COPUOS, and in addition a number of international organizations, including both intergovernmental and nongovernmental entities, have observer status in the Committee. COPUOS and its subcommittees function on the basis of consensus.

### Initial Scientific Policies

The Planetary Protection Policy began as a means of self-regulation by the international scientific community and pre-dated any applicable international law. In 1958, within months of the launch of Sputnik I, the ICSU formed the *Ad Hoc* Committee on Contamination by Extraterrestrial Exploration (CETEX), which considered celestial bodies to be scientific preserves. CETEX identified four primary objectives:

- (i) Freedom of exploration of celestial bodies, subject to limitations such as planetary quarantine requirements.
- (ii) Disclosure to COSPAR of information concerning activities and experiments.
- (iii) Only experiments which are likely to yield useful scientific data should be conducted.
- (iv) Nuclear explosions should not occur near the surface of celestial bodies (Tennen 2003/2004).

### Policies of Planetary Protection

In March 1962, Chairman Khrushchev of the Soviet Union drew the attention of the diplomatic community to the issue of protecting planetary environments. The Chairman wrote a letter to President Kennedy about what he described as "heavenly matters" and proposed that:

in carrying out experiments in outer space, *no one should create obstacles* to the study and use of space for peaceful purposes by other States. . .any experiments in outer space which may *hinder the exploration* of space by other countries should be the subject of preliminary discussion and of an agreement. . . (emphasis added)

Khrushchev inextricably linked protection of celestial environments to the right of states to conduct activities in the exploration and use of outer space. His focus, however, was not on the intrinsic value of preserving pristine celestial environments. Rather Khrushchev asserted and sought to protect the right of states to conduct activities in space without hindrance created by the activities of other states. He proposed that there should be a right to prior consent over activities and experiments of other states (Jakhu and Pelton 2017).

These and other issues were subject to debate and discussion in COPUOS, which recognized that the problem of preventing potentially harmful interference in the peaceful uses of outer space was of urgent concern. On November 22, 1963, COPUOS unanimously approved the Declaration of Legal Principles Governing the Activities of States in the Exploration and Use of Outer Space. The General Assembly of the United Nations thereafter adopted the Declaration of Principles as Resolution 1962. Planetary protection concerns were addressed in Paragraph 6:

In the exploration and use of outer space, States shall be guided by the principle of co-operation and mutual assistance and shall conduct all their activities in outer space with *due regard for the corresponding interests of other States*. (emphasis added)

The Declaration further provided that a state which has reason to believe its activities or experiments may cause harmful interference with the activities of another state shall undertake appropriate consultations with such second state. Similarly, if a state believes its activities may be interfered with by the activities of another state, it could request such other state to participate in consultations. This first legal planetary protection standard approved by the community of nations confirmed the complex interplay between preservation of celestial environments from harmful contamination and due regard for the right of states to conduct activities on other worlds without harmful interference.

### **Scientific Regulation Through Planetary Quarantine Requirements**

Following the work of CETEX, the ICSU established the COSPAR Consultative Group on Potentially Harmful Effects of Space Experiments, which released a comprehensive Planetary Protection Policy in 1964. This policy established “planetary quarantine requirements” (PQR) which adopted a probabilistic approach to protecting pristine celestial environments (COSPAR 1964). That is, the PQR established limitations expressed as a probability that a spacecraft could contaminate a celestial environment. The probability of contamination (P(c)) by any mission was determined by the formula:

$$P(c) = mi(0) \cdot P(vt) \cdot P(uv) \cdot P(a) \cdot P(sa) \cdot P(r) \cdot P(g)$$

where

mi(O) Initial microbial burden (at launch, after decontamination)  
 P(vt) Probability of surviving space vacuum-temperature  
 P(uv) Probability of surviving ultraviolet space radiation  
 P(a) Probability of arriving at planet  
 P(sa) Probability of surviving atmospheric entry  
 P(r) Probability of release  
 P(g) Probability of growth

The PQR set a probability limit for an accidental planetary impact by an unsterilized flyby or orbiting spacecraft to be  $3 \times 10^{-5}$  or less ( $< 1/300,000$ ). Spacecraft which were intended to penetrate the atmosphere or land on the surface of a planet were subject to a much higher standard. For these spacecraft, the probability limit for contamination by a single viable terrestrial organism aboard the craft was to be less than  $1 \times 10^{-4}$  ( $< 1/10,000$ ). These P(c) limits were to apply for an initial period of planetary exploration of 10 years, later extended to 30 years (Phillips 1975).

In 1966 the P(c) limit for landing or atmospheric penetration spacecraft was reduced to  $1 \times 10^{-3}$  (1/1000). This probability limit was an aggregate for all missions from all nations, and individual countries were allocated specific portions of the overall probability limits. The recipient states, in turn, apportioned their share among the various missions each conducted. The overall P(c) limits were divided as follows (Meltzer 2012):

USA	$4.4 \times 10^{-4}$
USSR	$4.4 \times 10^{-4}$
All others	$1.2 \times 10^{-4}$
Total	$1 \times 10^{-3}$

The United States, in turn, distributed its national allotment to the following interplanetary missions (Sterns and Tennen 2019):

Mariner Mars	$7.1 \times 10^{-5}$
Pioneer Jupiter	$6.4 \times 10^{-5}$
Mariner Venus	$7 \times 10^{-5}$
Viking	$2 \times 10^{-4}$ ( $1 \times 10^{-4}$ for each of two missions)

Compliance with the PQR generally required missions to engage in active decontamination techniques to reduce the presence of microbes on the spacecraft at launch. States employ a variety of techniques for this purpose. Prevention and limitation of the initial microbial burden are achieved by assembly and testing of a spacecraft in biologically controlled cleanrooms. The bioburden is reduced by cleaning with various solvents and by dry heat, plasma, or ionizing radiation. Barrier systems such as purging, filters, and seals are utilized to avoid possible re-contamination of the spacecraft. However, absolute sterilization of a spacecraft is not considered possible (Meltzer 2012).

## **Planetary Protection and the Emergence of Binding International Law**

The legal regulation of activities in space entered a new phase when COPUOS reached consensus on the text of the Treaty on Principles Governing the Activities of States in the Exploration and Use of Outer Space, including the Moon and Other Celestial Bodies (OST), which entered into force in October 1967. Article I of the OST recognizes the right of states to conduct peaceful activities on all areas of the Moon and other celestial bodies. Article IX of the treaty incorporated the due regard and consultation provisions of GA Res. 1962, the Declaration of Principles. In addition, and significantly, Article IX went further and explicitly addressed planetary protection and provided that in pursuing studies and conducting exploration of celestial bodies, states shall:

avoid their harmful contamination and also adverse changes to the environment of the Earth resulting from the introduction of extraterrestrial matter and, where necessary, shall adopt appropriate measures for this purpose.

Article IX is very broad in its terms and encompasses not just the concepts of due regard for, and the prevention of, harmful interference with activities of other states but also the inherent value in the preservation of natural celestial environments from harmful contamination. Nevertheless, there is no international consensus on the definitions of “harmful contamination” or “interference.” Nor have the interests of other states that shall be given due regard been identified, other than avoidance of harmful contamination. However, the COSPAR PPP represents a consensus that, at a minimum, harmful contamination includes the introduction of biological matter from the Earth into at least certain celestial environments.

## **Revisions to the PQR**

The COSPAR Planetary Protection Policy has not been static but rather has been subject to continuing review and revision. Within COSPAR is a recognized process by which changes to the policy can be considered, evaluated, and examined by pertinent stakeholders, including scientific commissions of COSPAR and members of the international planetary science community (Coustenis et al. 2019). As part of this process, the probabilistic approach on which the PQR was based was criticized for the inherent difficulty of assigning specific numerical values to criteria with largely unknown properties in order to determine the probability of contamination for a mission. Recognizing this difficulty in application of the PQR, COSPAR in 1969 limited the policy to missions to Mars and other planets deemed important in the search for extraterrestrial life (Stabekis 2002).

This change in the application of the policy was a significant departure from manner in which the risk of contamination to a celestial environment was viewed. The PQR proceeded from the original perspective articulated by CETEX that celestial bodies were scientific preserves, and as such the PQR were presumed to



be applicable to all interplanetary missions. The revisions to the PPP, however, limited the applicability of the decontamination requirements to only a small subset of interplanetary missions.

Subsequent revisions to the policy reinforced this change in perspective. For example, in 1978, the probability that terrestrial organisms could grow in extraterrestrial environments was re-evaluated and deemed to be virtually zero for most celestial bodies (Space Science Board 1978). As a result, requirements that missions to those bodies engage in active decontamination techniques were largely eliminated. The movement away from the probabilistic approach turned protection of celestial environments from a comprehensive blanket policy to one of restricted application. That is, PQR became the exception, not the norm, and active decontamination techniques would not be required for missions to alien worlds deemed too hostile for terrestrial microbes to survive and replicate.

## The Moon Agreement and Elaboration of Legal Regulation

In 1979 COPUOS achieved consensus on a second treaty which addressed forward and back contamination, the Moon Agreement (MA), which provides, in Article 7.1:

In exploring and using the Moon, States Parties *shall take measures to prevent the disruption of the existing balance of its environment* whether by introducing adverse changes in that environment, by its harmful contamination through the introduction of extra-environmental matter or otherwise. States Parties shall also take measures to avoid harmfully affecting the environment of the Earth through the introduction of extraterrestrial matter or otherwise. (emphasis added)

The obligations of states under the MA are more extensive than required by the OST. While the MA prohibits harmful contamination, as does the OST, the MA also prohibits states from disrupting the existing balance of the lunar environment. (Pursuant to Article 1.1 the provisions of the MA apply to other celestial bodies in the Solar System unless specific legal norms enter into force for such objects.) The MA makes it clear that environmental disruption could occur by several means, including but not limited to harmful contamination by the introduction of extra-environmental biological and other matter.

Article 7 contains a further departure from the OST in paragraph 3, which provides that states shall notify the Secretary General of areas of the Moon with special scientific interest, so that consideration shall be given to the designation of an area as an “international scientific preserve.” Such areas shall be subject to “special protective arrangements to be agreed upon in consultation with the competent bodies of the United Nations.”

The Preamble to the MA reflects that the treaty was formulated, in part, to define and develop the provisions of the OST, thereby providing some clarification as to the meaning of Article IX. However, the MA has not received widespread acceptance by the community of nations. While the OST has been signed or ratified by more than 130 states, only 18 states have ratified the MA, and just 4 more have signed the

instrument. These include India and members of ESA including Belgium, France, the Netherlands, and Austria. These states must ensure that any mission to celestial bodies in which they participate is conducted in compliance with their international obligations, including the MA (Jakhu and Pelton 2017).

## **Transformation of the PQR**

The derogation of the PQR continued into the 1980s, when the requirements were replaced with a new approach that provided the imposition of planetary protection constraints would be dependent upon the nature of the mission and the target body or bodies to be explored. These guidelines completely eliminated the overall probability of contamination restrictions and did not require any decontamination techniques or documentation for target bodies which were deemed not to be of biological interest in the search for life, including the Moon. The planetary protection classification for missions to other target bodies was to be determined on a case-by-case basis (Stabekis 2002).

Subsequent revisions continued to erode and limit the application of the PPP. In addition to the prerequisite conditions that a target body be both biologically interesting and deemed to provide an environment in which terrestrial microbes could survive and replicate, a third condition was added: that the mission spacecraft must include experiments intended to detect evidence of extraterrestrial life. An exception to this condition has been carved out for missions to areas of a celestial body which are designated as a “special region,” that is, an area which possesses properties which are known to be conducive to sustaining life in terms of temperature range and the presence of water. Spacecraft intended to land or explore or create (even temporarily by the operation of spacecraft hardware) a special region must achieve Viking-level decontamination, even where the mission does not include life detection experiments. However, the designation of an area as a special region under the PPP is not to be considered as the equivalent to an international scientific preserve pursuant to Article 7.3 of the MA. Special regions are expressly defined in relation to the search for evidence of indigenous life, while the designation as a scientific preserve is not limited to this purpose.

---

## **Current COSPAR Planetary Protection Policy**

### **Categorization of Target Bodies**

The overarching policy is stated by COSPAR as follows (COSPAR 2017):

The conduct of scientific investigations of possible extraterrestrial life forms, precursors, and remnants must not be jeopardized. In addition, the Earth must be protected from the potential hazard posed by extraterrestrial matter carried by a spacecraft returning from an interplanetary mission. Therefore, for certain space mission/target planet combinations,

controls on contamination shall be imposed in accordance with issuances implementing this policy

The implementation of the policy divides celestial bodies and mission types into four categories, with a fifth category designated for the return of extraterrestrial materials to the Earth. The concern for contamination and the concomitant contamination controls vary by category.

## Categories I and II

Category I consists of flyby, orbiter, and landing missions to target bodies which are not considered to be of significant interest in the search for life, such as Io and undifferentiated, metamorphosed asteroids. No specific PPP requirements are imposed for such mission/target body combinations.

Category II consists of flyby, orbiter, and landing missions to most of the moons in the solar system, including the Moon of the Earth, the planets – including Pluto – other than Mars, carbonaceous chondrite asteroids, comets, and some Kuiper belt objects. These target bodies are considered to be of “significant interest relative to the process of chemical evolution and the origin of life, but where there is only a remote chance that contamination carried by a spacecraft could compromise future investigations.” The term “remote” in this context “implies the absence of environments where terrestrial organisms could *survive and replicate*.. . (emphasis added).” Category II missions are subject to only simple documentation requirements, consisting of “a short planetary protection plan” identifying possible impact sites, brief pre- and post-launch analyses of impact strategies, and a post-encounter or mission report providing the location of any impact which occurred.

## Category III: Flyby and Orbiter Mission to Mars, Europa, and Enceladus

Category III target bodies are of both significant interest in the search for evidence of life and carry a significant chance that contamination could compromise future investigations. Since these missions are not intended to impact the target body, the policy allows for the spacecraft to satisfy a requirement of either orbital lifetime parameters or bioburden reduction. Orbital lifetime parameters require a probability of greater than or equal to 99% that the spacecraft will not impact the target body within 20 years of launch and greater than or equal to 95% on non-impact within 50 years. The bioburden reduction requirements limit the total number of spores on and in the spacecraft to less than or equal to  $5 \times 10^5$  (Spores are defined as aerobic microorganisms that survive a heat shock of 80 °C for 15 min and cultured on Tryptic-Soy-Agar at 32 °C for 72 h).

## **Category IV: Lander Missions to Mars, Europa, and Enceladus**

Category IV for landing craft is divided into three subcategories, depending on the mission type and objectives. Subcategory IV(a) applies to spacecraft which do not carry instruments designed to search for extant life. These spacecraft must meet bioburden limits of a total of less than or equal to  $3 \times 10^5$  spores and an average of not more than 300 spores per square meter.

Category IV(b) missions are designed to search for extant extraterrestrial life. Such missions are required to meet bioburden reduction levels four orders of magnitude more stringent than for Category IV(a) spacecraft, that is, a total of 30 spores, or the “levels of bioburden reduction driven by the nature and sensitivity of the particular life detection experiments.” However, if the life detection experiment hardware is cleaned to this level and the spacecraft is designed to ensure that the hardware cannot be exposed to possible recontamination, the remainder of the spacecraft can satisfy the PPP by meeting Category IV(a) limits.

Category IV(c) is for missions to special regions. Spacecraft landing within a special region must comply with Category IV(b) limits. If the special region is accessed through horizontal or vertical mobility, either the entire spacecraft or the subsystems which will encounter the special region must reach that level of cleanliness, and in the event of the latter, the subsystems must be designed to prevent recontamination after the bioburden is reduced.

## **Category V Sample Return Missions**

The four mission type/target body categories described above are concerned with forward contamination. The issue of back contamination is addressed in Category V, which applies to sample return missions. These sample return missions are classified as either restricted or nonrestricted. Missions to the Moon or Venus are nonrestricted Earth return and do not require any specific decontamination measures to be utilized. However, missions returning samples from Mars or Europa are restricted Earth return and warrant the highest level of caution to protect the Earth from potentially catastrophic contamination. (The importance of protective measures from potential back contamination is undeniably demonstrated by the Covid-19 health crisis which is devastating the globe as this chapter is in preparation.)

The PPP requires that the outbound leg of a restricted Earth return mission follow Category IV(b) requirements, to guard against “false positives” in experiments searching for extraterrestrial life. Unless the samples are to be sterilized prior to return to the Earth, the samples are to be kept in closed containers and a means provided to “break the chain of contact” with the target body. The PPP further provides that mission reviews and approvals are to be conducted at three stages: prior to launch from the Earth, after sample collection and before maneuvers to enter a biased Earth return trajectory, and prior to commitment to Earth reentry. In addition, unsterilized samples are either to be sterilized or subject to a program of life

detection and biohazard testing, as an absolute precondition to the controlled distribution of any portion of the sample.

In 2019, in response to a request from JAXA for guidance, the COSPAR PP Panel recommended that sample return missions to Phobos and Deimos be designated as nonrestricted Earth return (Coustenis et al. 2019). Samples to be returned from other small bodies in the solar system, which are not otherwise categorized, are to be designated as restricted or nonrestricted on a case-by-case basis. The criteria for this determination are set out in the PPP, as a series of questions:

1. Does the preponderance of scientific evidence indicate that there was never liquid water in or on the target body?
2. Does the preponderance of scientific evidence indicate that metabolically useful energy sources were never present?
3. Does the preponderance of scientific evidence indicate that there was never sufficient organic matter (or CO<sub>2</sub> or carbonates and an appropriate source of reducing equivalents) in or on the target body to support life?
4. Does the preponderance of scientific evidence indicate that subsequent to the disappearance of liquid water, the target body has been subjected to extreme temperatures (i.e., >160 °C)?
5. Does the preponderance of scientific evidence indicate that there is or was sufficient radiation for biological sterilization of terrestrial life forms?
6. Does the preponderance of scientific evidence indicate that there has been a natural influx to the Earth, e.g., via meteorites, of material equivalent to a sample returned from the target body?

For containment procedures to be necessary (“restricted Earth return”), an answer of “no” or “uncertain” needs to be returned to all six questions.

The sample return missions which have been launched since Apollo have all been nonrestricted, as these missions to comets, asteroids, or Phobos were not intended to return samples from a body deemed capable of supporting life. This situation will soon change as NASA is preparing to launch the first restricted Earth return mission, Mars 2020. This mission is planned to land on the red planet in 2021 and includes the capability to collect 40 separate samples of Martian material for return to the Earth. Mars 2020 is not itself a sample return mission but only a precursor to an as of yet not fully defined future mission that will return the collected samples. Nevertheless, these samples are subject to the standards of restricted Earth return, and the protocols to be developed for containing, isolating, transporting, and investigating any such samples are not without current controversy (MSR Science Planning Group Report 2019).

## Human Missions to Mars

Robotic sample return missions such as Mars 2020 are a stepping stone to the eventual human exploration of the planet. Application of the COSPAR PPP is not

limited to robotic missions, although the introduction of crews into the equation considerably complicates matters. The PPP recognizes that it will not be possible for human explorers to operate in entirely closed systems, nor can exposure with Martian materials be avoided. Moreover, the limitations on the initial microbial burden transported by robotic spacecraft are inapposite and unsuitable for human missions, which “will carry microbial populations that will vary in both kind and quantity. . .” Accordingly, the PPP identifies specific implementation guidelines for human missions to Mars, including:

- The development of a comprehensive protocol for addressing forward and backward contamination concerns during all phases of a mission.
- Continuous monitoring and evaluation of microbes carried by a mission.
- The designation of a member of the crew with primary responsibility for implementing planetary protection provisions.
- A quarantine capability for the crew during and after the mission in case of potential contact with a Martian life form.
- Robotic precursors to evaluate whether or not a site should be characterized as a special region prior to crew access.
- Planetary protection requirements for human missions should be based on a conservative approach recognizing the lack of specific knowledge of the Martian environment, possible life, and the utility and efficacy of human support systems.
- Planetary protection requirements for subsequent missions should not be relaxed without scientific justification and consensus.

The development of the necessary policies and procedures will be able to draw upon the experience and precedent of the Apollo program, in particular in regard to the Lunar Receiving Laboratory. The astronauts of Apollo 11, 12, and 14 were subject to quarantine upon their return from the Moon, as were the lunar materials they brought back to the Earth, until it was determined that they had not been exposed to harmful extraterrestrial contamination. It is known that the microbe *Microbispora* survived the harsh conditions of the ill-fated reentry of Columbia, (McLeana et al. 2006), and the possibility exists that terrestrial organisms can mutate in space and present new dangers. The lessons of Apollo can be instructive from technical, operational, and management perspectives, as issues were encountered in each area that resulted in certain breaks in the biological barrier that must not be repeated with Martian materials (Mangus and Larsen 2004).

---

## **Implementation of the COSPAR PPP by Space Agencies and Authorities**

The COSPAR PPP requirements do not have the force of binding law as they are neither a treaty nor a formal intergovernmental agreement. The specific requirements set forth in the PPP are more in the nature of guidelines rather than compulsory

obligations, and COSPAR does not direct the manner in which competent national authorities and international agencies can implement the policy. States which launch or register a spacecraft are internationally responsible and liable for the mission pursuant to the OST and have the duty to comply with Article IX to prevent the harmful contamination of celestial environments. COPUOS has recognized the PPP as the international reference standard for guiding compliance with Article IX of the OST in relation to contamination from biological sources (COPUOS 2017), but the PPP is not necessarily the only method by which states can comply with the treaty. Nevertheless, space active states generally have sought to satisfy the specific requirements articulated by COSPAR, and several agencies have incorporated the substantive provisions of the PPP into their formal governing documentation.

## **European Space Agency**

The Council of the European Space Agency (ESA) has adopted the “ESA Planetary Protection Policy.” The ESA PPP is implemented by specific “ESA Planetary Protection Requirements,” which are based on and consistent with the COSPAR PPP, and set forth the Agency’s overall planetary protection management responsibilities. These include technical requirements for robotic and human missions, requirements related to procedures, and descriptions of necessary documentation (Kminek 2017). In addition, this document contains internal ESA organizational descriptions and requirements. Neither the ESA PPP nor the ESA PPR have been released to the public. However, specific standards have been published by the European Cooperation for Space Standardization (ECSS) in “Space Sustainability – Planetary Protection” which are to be followed by ESA member states in their own projects. The ESA PPP and corresponding implementation standards apply to spaceflight missions conducted by ESA and to contributions to ESA spaceflight missions. Significantly, the ESA PPP also applies to ESA contributions to non-ESA spaceflight missions, such as missions conducted by other states, agencies, or the private sector which are launched by ESA or from ESA facilities.

## **The United States**

NASA has adopted NASA Policy Directive NPD 8020.7G, “Biological Contamination Control for Outbound and Inbound Planetary Spacecraft,” which mirrors the COSPAR policy statement.

The NPD is implemented by NASA Procedural Requirements NPR 8020.12D, “Planetary Protection Provisions for Robotic Extraterrestrial Missions,” which are based on and are in conformity with the COSPAR PPP. Pursuant to the NASA policy, the agency has established a Planetary Protection Officer, with responsibility to categorize missions and oversee compliance with the Planetary Protection Policy.

In 2017, NASA promulgated NASA Interim Directive NID 8020.109A, “Planetary Protection Provisions for Robotic Extraterrestrial Missions.” Section 2.2 of this

NID concerns NASA participation in non-NASA or non-US Missions, which assigns sole responsibility for planetary protection categorization and certification of compliance to the lead and launching organizations. Subsection 2.2.2 provides:

NASA shall provide hardware, services, data, funding, and other resources to non-NASA missions (including but not limited to resources agreements) only if the recipient organization(s), whether governmental or private entity, demonstrate adherence to appropriate policies, regulations, and laws regarding planetary protection that are generally consistent with the COSPAR Planetary Protection Policy and Guidelines

## **Japan**

Japan has launched several deep space explorations, including the Hayabusa 2 asteroid sample return mission currently in progress, without an overarching Planetary Protection Policy document in place. Nevertheless, individual projects implemented the COSPAR PPP by the adoption of conforming design standards and by achieving agreement with the COSPAR Planetary Protection Panel. Japan steadily has been increasing its space exploration activities, and in December 2018 JAXA established a planetary protection organization. Shortly thereafter, the agency issued a formal Planetary Protection Policy and associated requirements which are compliant with the COSPAR PPP, JAXA Management Requirement JMR-014, “Planetary Protection Program Standards.” These standards specify administrative, technical, and procedural aspects of planetary protection for both forward and back contamination. These standards apply to missions conducted by JAXA, parties who participate in missions conducted by JAXA, and JAXA’s participation in missions hosted by other organizations.

## **Russia**

The Russian Federal Law “On space activities” Decree No. 5663-1, Article 6, designates the State Corporation Roscosmos as the body authorized to ensure the safety of space activities. Article 4.1 provides that Roscosmos is responsible for ensuring that space activities are carried out in accordance with the principle of environmental protection. In order to ensure “strategic and ecological security,” Article 4.2 prohibits the creation of “harmful contamination of outer space which leads to unfavorable changes of the environment, . . .” This prohibition appears to be more limited than is Article IX of the OST, which expressly includes “the Moon and other celestial bodies” as part of outer space. The omission of specific reference to the Moon and other celestial bodies in this subsection of the Russian law indicates that it is directed only to the outer space environment, as another subsection expressly prohibits the use of the Moon and other celestial bodies for military purposes. In addition, the express direction that harmful contamination includes



the deliberate elimination or destruction of space objects in outer space implies objects in Earth orbit. Nevertheless, Article 26.3 affirms the duty of Russia to fulfill its obligations under the OST.

Russian Federal Laws “on technical regulation” No. 184-FZ, and “on sanitary and epidemiological well-being of the population” No. 52-FZ, address safety in general, including biological safety, but do not contain specific rules dedicated or directly addressed to issues of forward or back contamination. Nor apparently has Roscosmos publicly issued any official documents related to policies, procedures, or standards related to the biological protection of the Earth from the risks associated with space missions (Dobrokhotsky et al. 2012). However, missions such as Phobos-Grunt sample return were reviewed and approved as being in compliance with the COSPAR PPP, although the reliability of such certification can be questioned (Sterns and Tennen 2019).

## **Israel**

Israel has conducted a lunar mission and is planning future missions but does not have a publicly available formal Planetary Protection Policy governing document. The Israel IL lunar landing craft Beresheet was launched on a private American rocket from a NASA launch facility in Florida. As such, per NASA NID 8020.109A, the craft was subject to the NASA policy and requirements as set forth in NPD 8020.7G and NPR 8020.12D. Beresheet crashed on the lunar surface while attempting to land. Several months later reports began to circulate that a payload supplied by a third party had secretly encased some tardigrades, a primitive form of life, into some components that were carried to the Moon. A deliberate failure to disclose the presence of living organisms on a spacecraft launched to a celestial body would violate US law and policy (Johnson et al. 2019).

## **China/India/UAE**

China, India, and the UAE are each conducting missions to celestial bodies but do not have publicly available formal Planetary Protection Policy governing documents. The Chinese have a long history of space exploration, and have participated in COSPAR since 1993. China has sent four spacecraft to the Moon, the most recent of which is the Chang'e-4 that soft landed on the lunar far side in January, 2019, and continues to operate together with the Yutu-2 rover. China also sent a Martian orbiter, Yinghuo-1, and a microgravity grinding tool as payloads on the Phobos-Grunt mission. The Chinese plan to launch an orbiter and rover, Tianwen 1, to Mars in July 2020. Although an internal coordination mechanism has been implemented to formulate a relevant work plan for this mission, the Chinese are deferring formalizing a planetary protection policy pending further practice and research work.

The Indian Space Research Organization launched the Mars Orbiter Mission and the Chandrayaan mission to the Moon, and the agency followed the COSPAR policy

for both missions. ISRO currently is planning additional lunar and planetary missions and is in the process of preparing a formal Planetary Protection Policy. The UAE is preparing for the launch of the “Hope Probe” to Mars. The Emirates have embarked upon an ambitious program to become a significant participant in space activities. The UAE Space Agency is in the process of developing internal policies and procedures, including legal regulation; however it has not been publicly announced whether these policies, procedure, and regulations will include planetary protection considerations.

---

## Lacuna in the Planetary Protection Policy

The COSPAR PPP began as a comprehensive policy that recognized pristine celestial environments to be scientific preserves and established a Planetary Quarantine Policy applicable to all solar system bodies within our technological reach. Revisions to the policy have narrowed the scope and excluded celestial objects based on scientific explorations and results, new perspectives and approaches to planetary protection, and conclusions drawn regarding the biological interest of particular alien environments vis-a-vis the impact of the introduction of terrestrial organic matter and the ability vel non of terrestrial microbes to survive and replicate in such environments. As the COSPAR PP Panel reviews and re-evaluates the policy, consideration should be given to filling the gaps that remain, including the following:

### Expand Target Bodies in Categories III and IV

The more recent revisions to the PPP have included Europa and Enceladus in the list of target bodies subject to heightened protective measures. Six additional potential ocean worlds have been identified which may support alien life: Titan, Ganymede, Triton, Dione, Callisto, and Pluto. In addition to Mars, recent reports have indicated that Venus also may have been a habitable planet for much of the history of the solar system, and life may be present today in her clouds (Wall 2018; NASA 2016). Even Mercury, which long was considered to be completely uninhabitable, has been discovered to have ice deposits in shielded craters just like the Moon (NASA 2012). These discoveries expand the universe of extraterrestrial environments which are of potential interest in understanding the process of chemical evolution or the origin of life in the solar system, yet few of these target bodies currently are categorized so as to require active protective measures. Nevertheless, each category of the PPP notes that additional bodies can be added to any category on a case-by-case basis.

Discoveries of extremophiles on this planet confirm that we must be prepared to encounter life as we do not know it or may not even be able to recognize. Indeed, it was only just over 40 years ago that cellular organisms were discovered to be composed of three distinct types of organisms – archaea, bacteria, and eukarya

(Woese and Fox 1977). The gaps in our knowledge are great, and assumptions must be continuously tested. We do know that the basic building blocks of life are not unique to this planet and that once life takes hold, it grabs on tenaciously. It is not possible to conclude that life, or its precursors, could not have been or is not present in environments previously considered inhospitable if not antithetical to life without first conducting specific and thorough scientific investigations.

## **Missions to Phobos and Deimos Can Increase the Risk of Contaminating Mars**

The categorization of target bodies in the COSPAR PPP has a consequence which may have been unintended but nevertheless places certain celestial objects at increased and unnecessary risk of contamination. Specifically, a focus on a target body fails to adequately consider other bodies that may be within its relative vicinity. This gap within the PPP is illustrated by the Phobos-Grunt mission, which was conducted by the Russian Space Agency in 2011. The mission was intended to land a spacecraft on Phobos, which orbits less than 6000 km above the surface of Mars, collect samples of surface dirt and rocks, and return them to the Earth. The landing craft included a “bioshield module” provided by the Planetary Society, an American public advocacy organization. Called the “Living Interplanetary Flight Experiment (LIFE)” Project, the bioshield held 11 types of organisms from all three domains of life. These organisms ranged from the “mundane” to the “bizarre” and included extremophiles that were resistant to radiation, desiccation, salt, and heat. The Life Project sought to test the transpermia hypothesis, that is, whether a living organism could survive inside a meteorite and travel from planet to planet.

Phobos is considered to have an environment with a remote chance that terrestrial organisms could survive or replicate and therefore did not require stringent decontamination according to the COSPAR PPP. However, the Life Project BioShield enclosure was specifically designed to enhance and promote the survivability and replication of the organisms housed therein, negating the rationale which underlies Category II classifications.

There is no question but that the intentional introduction of potentially contaminating organisms within 6,000 km of Mars placed the planet at increased and unnecessary risk of despoiling the environment. Missions to Mars are difficult at best, and sample return missions are inherently more complex and challenging than a flyby, orbiting, or landing mission. The possibilities for a spacecraft off-nominal occurrence on or near Phobos are numerous, especially while engaging in arrival, landing, and return maneuvers, any one of which could result in an unintended and uncontrolled encounter with the Martian environment. Such accidental encounters could occur anywhere on the planet, including in special regions.

The launch of the LIFE Project failed to adequately consider the risk to the Martian environment and neither represented the best practice of states nor established good precedent. The mission ended when the spacecraft failed to leave

Earth orbit and fell back into the atmosphere and burned up. As a matter of due regard, the PPP should strictly scrutinize any proposed experiment that increases the risk of harmful contamination to a celestial environment, even if it is not the intended target body. Justification for such a mission must demand that the scientific results sought to be attained are of a very high significance and are not available by any other alternative means (Sterns and Tennen 2019).

## **Challenges to Planetary Protection by Private Sector Commercial Projects**

Additional gaps in the COSPAR PPP are presented by the emergence of New Space commercial ventures. The OST provides in Article VI that states are internationally responsible for the activities of their nationals in space and that nongovernmental entities must be authorized and continuously supervised by their appropriate state. Neither ESA, NASA, nor JAXA authorize private sector activities, and as noted above, the agencies have adopted policies which require adherence with their planetary protection policies for any missions in which they participate. This includes commercial missions; however private sector activities without ESA, NASA, or JAXA participation are not subject to those agencies' internal policy requirement documents. Several states have adopted or are in the process of drafting national licensing regimes for the authorization and supervision of New Space activities (Jakhu and Pelton 2017). However, to date none of these national regimes has included specific reference to, or a requirement to comply with, the COSPAR PPP or similar strictures (Babb et al. 2018).

The COSPAR PPP does not address the implications and ramifications of the discovery of evidence of alien life. The scientific community presumably would take all necessary steps to protect and preserve the evidence and proceed with additional experimentation and exploration with the utmost care. The motivations of the private sector, however, are not necessarily congruent with scientific investigation. Therefore, it is imperative that the Planetary Protection Policy considers the adoption of rules and procedures for the private sector to follow in the event of discovery of evidence of alien life, or the remnants or precursors thereof, or other discoveries of scientific interest.

Policies will need to be developed regarding the disclosure of a discovery of evidence of extraterrestrial life. This would be consistent with the provisions of Article 5.3 of the MA which obligates states to disclose the discovery of any indication of organic life. This disclosure is to be made to the Secretary General, the international scientific community, and the public at large. Private sector ventures may be hesitant to make such a disclosure, especially if there is the possibility of obtaining a financial opportunity from intellectual property rights derived from a non-terrestrial microbe (Long 2016).

The area in proximity to a discovery of extraterrestrial life, and other discoveries of scientific interest, must also be protected and preserved. In addition, it must be determined whether commercial activities should be prohibited from conducting

resource extraction and other activities from areas of special scientific interest, such as special regions on Mars, pending further scientific investigation (Sterns and Tennen 2019).

Commercial activities present additional issues from a planetary protection perspective, such as the need for the scientific community to be informed of and have the opportunity to express any concerns about proposed missions prior to the issuance of licenses or other authorizations. Private sector missions should be required to disclose an inventory of hazardous materials carried on a spacecraft and provide pre- and post-mission environmental impact assessments for activities conducted in situ.

The focus of the COSPAR PPP on biological contamination is only one aspect of the impact New Space ventures will have on celestial environments. The regulation of the private sector in space will need to consider planetary environmental protection more broadly, such as what requirements, if any, should be imposed on commercial ventures to restore the surface and subsurface of celestial bodies and remove private spacecraft and other objects at the end of their operations. Moreover, historic sites and other unique locations of special interest should be protected from being despoiled in the name of profit.

Whether or not an area has particular historical or scientific interest, appropriate regulation of the private sector will need to consider limitations and prohibitions on materials that can be transported on board a spacecraft and deposited on a celestial object. Commercial ventures have already begun to market the “service” of lunar “burial” of human remains and to carry almost unlimited personal objects on board a landing craft to establish a permanent monument on the Moon. In addition to the obvious environmental impact, erecting shrines to vanity and littering the lunar surface with useless detritus violate any number of provisions of international law, including the non-appropriation principle in Article II of the OST. These commercial ventures harken back to the concerns expressed by Khrushchev in 1962 about activities that create obstacles and hinder the activities of others. The creation of obstacles and hindrances is inherently provocative and destabilizing to space security.

---

## Conclusion

The protection of celestial environments presents scientific, legal, ethical, moral, aesthetic, and philosophical considerations (Rummel et al. 2012). COSPAR has been the leading scientific organization to articulate and develop a policy of planetary protection, which has been recognized as the international standard for compliance with Article IX of the OST regarding protecting against forward and back contamination from biological sources. The COSPAR PPP promotes space security by furthering the interests of science and enhancing the essential goal of international space law to safeguard space, including the Moon and other celestial bodies, for peaceful exploration and use by all states.

## References

- Babb RJ, Erb H, Howard D (2018) Cost reduction solutions in regard to PP for commercial companies, IAF Paper No. IAC-18-F1.2.3
- COSPAR Planetary Protection Policy, Space Research Today, No. 200, p. 12 (2017). <https://cosparhq.cnes.fr/assets/uploads/2019/12/PPPolicyDecember-2017.pdf>. Last accessed February 29 2020
- Coustenis A, Kminek G, Hedman N, Ammannito E, Deshevaya E, Doran PT, Grasset O, Hayes A, Lei L, Nakamura A, Prieto-Ballesteros O, Raulin F, Rettberg P, Sreekumar P, Tsuneta S, Viso M, Zaitsev M, Zorzano-Mier P (2019) The COSPAR panel on planetary protection role, structure and activities. [https://cosparhq.cnes.fr/assets/uploads/2019/07/PPP\\_SRT-Article\\_Role-Structure\\_Aug-2019.pdf](https://cosparhq.cnes.fr/assets/uploads/2019/07/PPP_SRT-Article_Role-Structure_Aug-2019.pdf). Last accessed February 29 2020
- Dobrokhotzky ON, Dyatlov IA, Orlov OI, Novikova ND, Hamidullina NM, Deshevaya EA (2012) Ensuring biosafety in the study of samples of extraterrestrial origin by an example of preparation for the “Phobos-Grunt” Mission. <https://cyberleninka.ru/article/n/obespechenie-biologicheskoy-bezopasnosti-pri-issledovanii-materialov-vnezemnogo-proishozhdeniya-na-primere-podgotovki-ekspeditsii/viewer> (in Russian). Last accessed February 29 2020
- Hofmann M, Retberg P, Williamson M (eds) (2010) Protecting the environment of celestial bodies: the need for policy and guidelines jaxa jmr-014, the planetary protection standards. <http://sma.jaxa.jp/TechDoc/Docs/JAXA-JMR-014.pdf> (in Japanese). Last accessed February 29 2020
- Jakhu RS, Pelton JN (eds) (2017) Global space governance: an International study 389, 392, 453–54
- Johnson CD, Porras D, Hearsay CM and O’Sullivan S (2019) The curious case of the transgressing tardigrades (part 2). <https://www.thespacereview.com/article/3786/1>. Last accessed February 29 2020
- Kminek G (2017) Planetary Protection at ESA. <http://pposs.org/wp-content/uploads/2017/03/7.-PPOSS-PP-at-ESA-G.-Kminek.pdf>. Last accessed February 29 2020
- Long GA (2016) The meaning of life and close encounters of the commercial kind, 2015 proceedings of the international institute of space law 175
- Mangus S, Larsen W (2004) Lunar receiving laboratory project history [https://www.lpi.usra.edu/lunar/documents/lunarReceivingLabCr2004\\_208938.pdf](https://www.lpi.usra.edu/lunar/documents/lunarReceivingLabCr2004_208938.pdf). Last accessed February 29 2020
- McLeana RJC, Welsha AK, Casasanto VA (2006) Microbial survival in space shuttle crash. *Icarus* 181(1):323–325
- Meltzer M (2012) When biospheres collide: a history of nasa’s planetary protection programs 82 [http://www.nasa.gov/connect/ebooks/when\\_biospheres\\_collide\\_detail.html](http://www.nasa.gov/connect/ebooks/when_biospheres_collide_detail.html). Last accessed February 29 2020
- MSR Science Planning Group (2019) Science-driven contamination control issues associated with the receiving and initial processing of the msr samples. <https://mepag.jpl.nasa.gov/reports.cfm>. Last accessed February 29 2020
- NASA (2012) Messenger finds new evidence for water ice at mercury’s poles [https://www.nasa.gov/mission\\_pages/messenger/media/PressConf20121129.html](https://www.nasa.gov/mission_pages/messenger/media/PressConf20121129.html). Last accessed February 29 2020
- NASA (2016) NASA climate modeling suggests venus may have been habitable. <https://www.nasa.gov/feature/goddard/2016/nasa-climate-modeling-suggests-venus-may-have-been-habitable>. Last accessed February 29 2020
- Phillips CR (1975) The planetary quarantine program: origins and achievements 37. <https://ntrs.nasa.gov/archive/nasa/casi.ntrs.nasa.gov/19750006598.pdf>. Last accessed February 29 2020
- Rummel JD, Race MS, Horneck G (2012) Ethical considerations for planetary protection in space exploration: a workshop. *Astrobiology* 12(11):1017–1023
- Space Science Board Committee on Planetary Biology and Chemical Evolution (1978) Recommendations on Quarantine Policy for Mars, Jupiter, Saturn, Uranus, Neptune and Titan 27–28 (Appendix C)
- Stabekis P (2002) History and processing of changes, in report, COSPAR/IAU Workshop on planetary protection (Appendix C)

- Sterns PM, Tennen LI (2019) Lacuna in the updated planetary protection policy and international law, 23 life sciences in space research 10 <https://www.sciencedirect.com/science/article/pii/S2214552418301007>. Last accessed February 29 2020
- Tennen LI, Evolution of the planetary protection policy: conflict of science and jurisprudence? Proceedings of the 45th colloquium on the law of outer space 466 (2003) and Advances in Space Research 34 (2004): 2354–2362
- Wall M (2018) Life on venus? Why its not an absurd thought. <https://www.space.com/40304-venus-clouds-alien-life-search.html>. Last accessed February 29 2020
- Woese CR, Fox GE (1977) Phylogenetic structure of the prokaryotic domain: the primary kingdoms. Proc Natl Acad Sci U S A 74:5088–5090. <https://www.ncbi.nlm.nih.gov/pubmed/270744>. Last accessed February 29 2020

## Additional Reading

- Compendium on mechanisms adopted in relation to non-legally binding United Nations instruments on outer space, Submission by Japan, UN Doc. A/AC.105/C.2/2019/CRP.16 (2 April 2019). [http://www.unoosa.org/res/oosadoc/data/documents/2019/aac\\_105c\\_22019crp/aac\\_105c\\_22019crp\\_16\\_0\\_html/AC105\\_C2\\_2019\\_CRP16E.pdf](http://www.unoosa.org/res/oosadoc/data/documents/2019/aac_105c_22019crp/aac_105c_22019crp_16_0_html/AC105_C2_2019_CRP16E.pdf). Last accessed February 29 2020
- European Cooperation for Space Standardization (ECSS) (1 August 2019) Space Sustainability – Planetary Protection, ECSS-U-ST-20C. <https://ecss.nl/standard/ecss-u-st-20c-space-sustainability-planetary-protection>. Last accessed February 29 2020
- Hofmann M, Retberg P, Williamson M (eds) (2010) Protecting the environment of celestial bodies: the need for policy and guidelines jaxa jmr-014, the planetary protection standards. <http://sma.jaxa.jp/TechDoc/Docs/JAXA-JMR-014.pdf> (in Japanese). Last accessed February 29 2020
- NASA Interim Directive NID 8020.109A, Planetary Protection Provisions for Robotic Extraterrestrial Missions. [https://nodis3.gsfc.nasa.gov/OPD\\_docs/NID\\_8020\\_109A.pdf](https://nodis3.gsfc.nasa.gov/OPD_docs/NID_8020_109A.pdf). Last accessed February 29 2020
- NASA Policy Directive NPD 8020.7G, Biological Contamination Control for Outbound and Inbound Planetary Spacecraft. <https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPD&c=8020&s=7G>. Last accessed February 29 2020
- NASA Procedural Requirements NPR 8020.12D, planetary Protection Provisions For Robotic Extraterrestrial Missions, <https://nodis3.gsfc.nasa.gov/displayDir.cfm?t=NPR&c=8020&s=12D>. Last accessed February 29 2020
- Russian Federal Law “On space activities” Decree No. 5663-1 [http://www.unoosa.org/oosa/en/ourwork/spacelaw/nationalspacelaw/russian\\_federation/decree\\_5663-1\\_E.html](http://www.unoosa.org/oosa/en/ourwork/spacelaw/nationalspacelaw/russian_federation/decree_5663-1_E.html). Last accessed February 29 2020

---

# Index

## A

- Acceptable safety levels, 269–270
- Active debris removal (ADR), 214, 280, 313–314
- agent-based ground network, 1054
  - and insurance strategy, 1055–1060
  - low Earth orbit (LEO), 1044
  - marketing model, satellite mega-constellation, 1050
  - medium Earth orbit (MEO), 1044
  - propagation, 1046
  - reliability simulation model for satellite constellation, 1045–1046
  - replenishments scenarios, 1049
  - validation, 1055
- Active defense, 534
- Active Layered Theatre Ballistic Missile Defence (ALTBMD) Program, 1236
- Aditya mission, 502
- Administrative License Law of the People's Republic of China, 522
- Advanced extremely high frequency (AEHF) satellites, 1138–1139
- SATCOM system, 788
- Advance publication information (API) procedure, 991, 992
- Aerospace Industries Association (AIA), 195
- Africa
- economic and financial (E&F) operations, 169
  - space activities in, 16–17
- African Postharvest Loss Information System (APHLIS), 762, 763
- Agricultural and water resources, exploitation of, 686–693
- Agriculture, postharvest loss reduction
- bi-directional information flows, 770
  - end-user interfaces, 768–769
  - geonavigation, 765
  - historical data and real-time data, 770
  - information transmission, 765–766
  - infrastructure, 767–768
  - integrated decision support algorithms, 770
  - knowledge and skills, 767
  - legal, political and economic considerations, 773–774
  - pricing of goods, 771
  - remote sensing imagery and environmental data, 764–766
  - route optimization, 766
  - system efficiency, integration and optimization, 761–764
  - system interoperability, 768
  - system maintenance and upgrades, 769
- Agriculture value chain, 764–766
- Airborne Warning and Control System (AWACS), 582
- Air Defense and Air Operations Command (CDAOA), 1335
- Air Defense Artillery (ADA), 372
- Airport Authority of India (AAI), 1429
- Air traffic management (ATM), 947, 948, 950
- Alcantara Launching Center (CLA), 657
- Alliance Ground Surveillance (AGS), 1216, 1217
- Al Yah Satellite Communication Company, 640
- Ambiguous symbolism, 40
- Amos-6, 594
- Androgynous docking system (APAS), 296
- Angara, 1174
- Annihilation/destruction effect, 873
- Antarctica, economic and financial (E&F) operations, 174
- Antarctic Treaty, 77
- Anthropocene age, 1029
- Anti-Ballistic Missile (ABM) Treaty, 45, 63, 99, 374, 376, 389



- Anticipation, 137
- Anti-satellite (ASAT) test, 338, 360, 363, 533, 1081
- Anti-satellite (ASAT) weapons system, 4, 42–43
- Anti-satellite weapons tests (ASATs), 389, 390, 394, 396
- Antrix Corporation Limited (ANTRIX), 572, 579
- Apollo 11, 77
- Apollo 17, 1014
- Application programming interfaces (APIs), 768
- Arab Space Cooperation Group, 646
- Arctic state, economic and financial (E&F) operations, 173–174
- Ariane Passenger Payload Experiment (APPLE), 1424
- Arichtarchos Telescope, 1306
- Armored space systems, 871
- Arms control
  - agreements, 38
  - in outer space, 99–102
  - Partial Test Ban Treaty, 99
  - SALTII, 100
  - treaty, 43–45
  - UN General Assembly, 100–102
- Arms Export Control Act (AECA), 198
- Arnhem Space Centre project, 1449
- ARTEMIS, 1230
- Artificial intelligence (AI), 709, 724, 771
- Artificial intelligence (AI) and space safety
  - ANN, 951–953
  - automation, 950
  - challenges, 955–956
  - decision-making stages, 951
  - disposal and re-entry stages, 955
  - engineering, 948–950
  - false alarms, 951
  - SVM, 951
- Artificial neural networks (ANN), 951–953
- Aryabhata, 1424
- Asia, 362
  - space activities in, 18
- Asia-Pacific Regional Space Agency Forum (APRSF), 563
- Assistant Secretary of the Air Force for Space Acquisition and Integration (ASecAF SA&I), 56
- Astrium Services (ASV), 1254
- Astropolitik: Classical Geopolitics in the Space Age, 52
- Athena-Fidus, 789, 1068
- Augmented Satellite Launch Vehicle (ASLV), 573, 1423, 1425
- Australia Group, 190
- Australia, space activities in, 20
- Australia's space security programme
  - Defence Integrated Investment Program, 1447–1448
  - defence policy, 1445–1447
  - dependence on space, 1443–1444
  - launches, 1449–1450
  - National security and space, 1444–1445
  - Next Generation Technologies Fund, 1448–1449
  - SmartSat CRC, 1451
- Austria, 426, 432, 434, 436, 438, 440
  - EO, ISR, 1267
  - PNT, 1268
  - SATCOM, 1268
  - space and security budget, 1267
  - SSA, 1268
- Austrian Research Promotion Agency, 426
- Austrian Space Applications Programme (ASAP), 1267
- Automated GNSS Network of Switzerland (AGNES), 1283
- Automated systems, 854
- Automated transfer vehicle (ATV), 871
- Aviation Industry Commission, 516
- Aviation Law, 519
- Azerbaijan, 361
- Azerbaijan National Aerospace Agency (ANASA), 362
- Azerbaijan, space and security activities
  - agricultural and water resources, exploitation of, 686–693
  - Azercosmos, 670–672
  - environmental damage, 674–679
  - natural resources, exploitation and pillage of, 679–685
  - permanent infrastructure changes, 675–682
  - permanent social infrastructure, implantation of settlers and construction of, 694
  - public and private property, destruction of, 682–688
  - satellite imagery sources and analysis methodology, 672–674
- Azercosmos, 670–672
- Azersky, 668, 670–673, 697
- Azerspace-2, 671

**B**

Baikunur Cosmodrome, 1181–1182  
 Balkan conflicts, 1502  
 Ballistic missile(s), 1012  
 Ballistic missile defense (BMD), 389, 395, 1215  
 Ballistic Missile Early Warning System (BMEWS), 1012  
 Basic Space Law, 556, 557, 561–564, 568, 569  
 Basic Space Plan, 363  
 Battle of Takur Ghar, 1015, 1016  
 BeiDou Navigation Satellite System (BDS), 178, 830, 912, 1389–1390, 1397  
 Beidou satellites, 805–806  
 Belgium  
   EO, ISR, 1269  
   PNT, 1270–1271  
   SATCOM, 1269–1270  
   space and security budget, 1268–1269  
   SSA, 1271  
 Belt and Road Initiative (BRI), 580, 1382, 1390, 1396, 1398  
 Berne Club, 442  
 Bhaskara-I, 1424  
 Bhaskara-II, 1424  
 Biological Weapons Convention (BWC), 190  
 Bogota Declaration, 78  
 Brazil, 364  
   space activities in, 25  
 Brazilian National Institute for Space Research (INPE), 663  
 Brazilian space law, 364  
 Brazilian space security  
   artificial satellites, 656  
   data law, 662  
   legislative structure, 659  
   PAROS, 664–665  
   policy, 656–658  
   space assets, 656  
   space certification body, 660–661  
   space law treaties, 655  
   space program, 658  
   space safety regulations, 659  
   space situational awareness, 662–664  
 British spacepower  
   capabilities, 1371–1377  
   communication satellites, 1372–1374  
   ISR and EO satellites, 1374–1375  
   launch, 1377  
   navigation, 1376–1377  
   space policy and strategy, 1368–1371  
   space situational awareness, 1374

Broadcasting-satellite service (BSS), 780, 994, 999  
 Burke, Arleigh, 372  
 Bush, George W., 376, 377

**C**

Canada, space activities in, 27  
 Capability Development Plan (CDP 2018), 826  
 Capsules, 288  
 Carbonite-2 live video imagery satellite, 1375  
 Carter, James, 375  
 Celestial bodies  
   current status quo, 344–345  
   evolution of space activities on, 348–354  
   weaponization of outer space, 345–348  
 Center for Strategic and International Studies (CSIS), 68  
 Centre for the Development of Industrial Technology (CDTI), 428  
 CERES program, 1235  
 Chandrayaan-1, 574, 577, 1430  
 Chang'e-4 relay satellite, 1389  
 Chemical Weapons Convention (CWC), 190  
 Chernobyl nuclear reactor accident, 406  
 Chief of Space Operations (CSO), 55  
 China, 362  
   economic and financial (E&F)  
     operations, 177  
   information dominance, 536–537  
   local wars under informationized conditions, 530–531  
   local wars under modern, high-technology conditions, 530  
   military leadership, 85  
   military planners, 528  
   military SATCOM, 793  
   new circumstances (*see* Information and communications technology (ICT))  
   PLA, 528  
   space activities in, 18  
   space capabilities, 528–533  
   space dominance, 537  
   space operations (*see* Military space operations)  
   space program, 85  
 China Aerospace Science and Industry Corporation (CASIC), 516, 533, 547, 1389  
 China Aerospace Science and Technology Corporation (CASC), 516, 532, 547, 1387, 1389, 1396

- China Brazil Earth Resources Satellite (CBERS), 532
- China-France Oceanography Satellite (CFOSat), 1398
- China High-resolution Earth Observation System (CHEOS), 1384–1385
- China National Space Administration (CNSA), 519
- China Seismo-Electromagnetic Satellite (CSES), 1393–1394
- China's launch vehicles  
 development, 1402–1403  
 international commercial launch record, 1406  
 LM (*see* Long March (LM) launch vehicles)  
 new generation, 1415–1416  
 planning, 1403  
 space security policy, 1417–1418
- China space industry  
 communication satellites, 910–912  
 history of, 906  
 policy advocates, 906  
 safety, 918  
 satellite navigation system, 912  
 space debris, 914
- China's space safety, international exchanges and cooperation on, 916–918
- China's space security  
 civil-military integration policy, 518–519  
 peaceful uses and exploration of outer space, 517–518  
 policy, 1419–1420  
 radio frequency management regime, 521–523  
 space debris mitigation measures, 520–521  
 space policy-making, 523–524
- Chinese Academy of Sciences (CAS), 1392, 1397
- Chinese anti-satellite (ASAT) test, 60, 305, 381
- Chinese BeiDou satellites, 639
- Chinese National Security Council, 65
- Chinese satellite program  
 CHEOS, 1385  
 commercial remote sensing satellites, 1386–1387  
 communications and broadcasting satellites, 1387–1389, 1396–1397  
 CSES, 1393–1394  
 DAMPE, 1392–1393  
 Double Star Program, 1392  
 environment and disaster monitoring and forecasting, small satellite constellation for, 1385  
 Fengyun, 1383  
 Gaofen, 1385  
 Haiyang, 1384  
 HXMT, 1393  
 international exchanges and cooperation, 1397–1399  
 navigation and positioning satellites, 1389–1390, 1397  
 QUESS, 1393–1394  
 satellite application phase, 1382  
 Shijian series, 1391  
 Strategic Priority Program on Space Science, 1392  
 technology preparation phase, 1382  
 technology test phase, 1382  
 Tianyuan-1, 1394  
 Yaogan, 1385  
 Ziyuan, 1384
- C3IEL, 594
- Civil-military integration, 547–549
- Civil-military integration policy, 518–519
- Civil space traffic management (CSTM), 315
- Clinton, William, 377
- CO3D program, 1229
- Cold War, 6, 74, 76, 80, 85, 214, 386, 390
- Collision avoidance (CA), 847, 853, 854, 856, 859  
 service, 895
- Collision avoidance manoeuvres (CAM), 943–946, 954
- Comets  
 cosmic hazards, 1029–1033  
 protective strategies for defense against, 1033–1034
- Command, Control, Communications, Computer, Intelligence, Surveillance and Reconnaissance (C4ISR), 701, 926
- Commerce Control List (CCL), 197
- Commercial earth observation, 910
- Commercially hosted infraRed payload (CHIRP), 1158
- Commercial-off-the-shelf (COTS), 929
- Commercial orbital transportation services (COTS) program, 1501
- Commercial SATCOM (COMSATCOM), 784
- Commercial space, 1528  
 activity, 66, 67
- Commercial space sector, 1480  
 launches in 2017, 1482  
 non-commercial and commercial launches, 1482

- Committee on Contamination by Extraterrestrial Exploration (CETEX), 1562
- Committee on Space Research (COSPAR), 1561
- Committee on the Peaceful Uses of Outer Space (COPUOS), 1084, 1094, 1096, 1562, 1572
- Common Commercial Policy (CCP), 201
- Common Foreign and Security Policy (CFSP), 201, 402, 403, 479, 1195, 1197
- Common heritage of mankind (CHM), 66
- Common Security and Defence Policy (CSDP), 473, 479, 1195
- Communication satellites, 702
- China, 910–912
- Communications intelligence (COMINT) satellite, 1159
- Communism, 557
- Compass/BeiDou Navigation Satellite System, 805–806
- Compellence, 113
- Complex supply chains, 929
- Complex system governance, 239–242
- Composante Spatiale Optique* (CSO), 1229
- Comprehensive document of aerospace development, 607–609
- Comprehensive Nuclear-Test-Ban Treaty (CTBT), 190
- Comprehensive scientific map of Iran, 606–607
- Computer systems, 248
- COMSATBw, 789
- Conference on Disarmament (CD), 88, 334, 346, 1539, 1542, 1547
- Subsidiary Body 3, 1548
- Working Group on the “Way Ahead”, 1547
- Conjunction assessment risk analysis (CARA), 945
- Conjunction data message (CDM), 944, 945
- Contamination, 345
- Contrario, 878
- Controlled Radiation Pattern Antennas (CRPA), 813
- Conventional radars, 976
- Convention on International Civil Aviation, 77
- Cooperation
- and capacity-building, 151–152
  - international, 146
  - Moon and space resources, 158–159
  - in outer space, 148
  - for safety and sustainability, 153–155
  - in space exploration, 149–151
  - space security, 146
  - space security vs. national security, 155–158
  - technical and utilitarian modes of, 148–149
- Co-orbital tests, 870
- Coordinated Annual Review on Defence (CARD), 1196
- Copernicus, 1198–1199, 1209–1210
- Copernicus Contributing Missions (CCMs), 1116
- Copernicus emergency management service, 735
- early warning, 745–746
  - rapid mapping service, 736–739
  - risk and recovery mapping service, 739–745
- Copernicus flagship program, 1507
- Copernicus programme, 719–723, 1096, 1109
- contributing mission data, 1116–1118
  - open access policy and security restrictions, 1111–1114
  - scope, 1111
  - Sentinel data, 1115–1116
- Copernicus Support to EU External Action (SEA), 721
- Coronal mass ejections (CMEs), 1008, 1010, 1035, 1037, 1038
- Cosmos 2251, 278
- Cosmos-Iridium collision, 60
- COSMO-SkyMed, 641, 1244, 1352
- COSPAR Planetary Protection Policy, 1568, 1576–1578
- categorization of target bodies, 1567–1568
  - China/India/UAE, 1574–1575
  - ESA, 1572
  - fly-by and orbiter mission to Mars, Europa and Enceladus, 1568
  - human missions to Mars, 1570–1571
  - Israel, 1574
  - Japan, 1573
  - lander missions to Mars, Europa and Enceladus, 1569
  - Russia, 1573–1574
  - sample return missions, 1569–1570
  - United States, 1572–1573
- Crew Module Atmospheric Reentry Experiment (CARE), 1434
- Critical infrastructure protection (CIP), 6, 228–231
- Critical space infrastructure
- critical space infrastructure protection, 234–236
  - vs. space infrastructure, 233–234
- Cross-border crime (CBC), 718
- Cross-country mobility analysis (CCM), 718
- Cryogenic Study Team, 575

- Cuban Missile Crisis, 74  
 CubeSat, 308, 942, 1152, 1445  
   constellations, 929  
 Cyber-attacks, 360, 703, 875–877, 1334  
 Cyber defense, 701–703  
 Cyber defense situation awareness  
   (CDSA), 930  
 Cyber security, 6, 217, 468, 701–703  
 Cybersecurity operations team, 933  
 Cyber Security Space Operations Centre  
   (CySOC), 930, 934  
 Cyberspace  
   assured access to, 922  
   challenges and recommended actions, 929  
   cyber defence convergence, 926–927  
   cyber defence technologies, 927  
   cyber threat landscape, 925–926  
   outer space and, 922  
   situation awareness (SA) concepts, 930  
   space security issues, 928  
   vulnerabilities, 923  
 Czech Republic  
   EO, ISR, 1292–1293  
   PNT, 1293–1294  
   SATCOM, 1293  
   space and security budget, 1292  
   SSA, 1294
- D**  
 Dark Matter Particle Explorer (DAMPE),  
   1392–1393, 1397  
 Data law, 662  
 DEAL Guadeloupe, 742  
 Deception, 117  
 Defence Action Plan, 1505  
 Defence Advanced GPS Receiver  
   (DAGR), 827  
 Defence Cooperative Research Centre  
   Program, 1449  
 Defence project 799, 1451  
 Defence Research and Development  
   Organisation (DRDO), 507, 573,  
   583, 584  
 Defence space programs, 1487  
 Defence Space Research Organisation  
   (DSRO), 507  
 Defense, 12  
 Defense Advanced Research Projects Agency  
   (DARPA), 831  
 Defense meteorological satellite program  
   (DMSP), 1162  
 Defense Space Agency, 503  
 Defense support program (DSP) satellites, 1155  
 Defensive space operations, 542–543  
 Democratic Party of Japan (DPJ), 561  
 Denmark  
   EO, ISR, 1295–1296  
   PNT, 1297  
   SATCOM, 1296–1297  
   space and security budget, 1294–1295  
   SSA, 1297–1298  
 Department for Business, Energy and Industrial  
   Strategy, 430  
 Department of Defense (DOD), 53, 368, 375,  
   377, 381  
 Detente, 870  
 Deterrence, 4  
 Dhawan, Satish, 573, 577  
 DigitalGlobe, 1154  
 Directed energy weapons (DEW), 872  
 Disaggregation, 117  
 Disaster management, 246  
 Disruption effect, 873  
 Distribution, 117  
 Diversification, 117  
 DLR Space Administration, 428  
 Dnepr, 1180  
 Dolman, Everett, 51  
 Double Star Program, 1392  
 Draft Treaty on Prevention of the Placement of  
   Weapons in Outer Space and of the  
   Threat, 102–106  
 Dual-usable assets, 39–41  
 Duchifat-1, 594  
 Duchifat-2, 594  
 Dutch Geodata for Agriculture and Water  
   (G4AW) program, 1272  
 Dyna-Soar Program, 373
- E**  
 Earth observation (EO), 215, 907, 1198–1201,  
   1208–1210, 1216–1217, 1428  
   Austria, 1267  
   Belgium, 1269  
   Czech Republic, 1292–1293  
   Denmark, 1295–1296  
   Estonia, 1298–1299  
   Finland, 1302–1303  
   France, 1227–1230  
   Germany, 1237–1241  
   Greece, 1305  
   Hungary, 1307–1308

- Ireland, 1309–1310
- Italy, 1244–1245
- Luxemburg, 1311–1312
- Norway, 1276
- Poland, 1314–1315
- Portugal, 1318–1319
- Romania, 1321–1323
- Spain, 1248–1250
- Sweden, 1280
- Switzerland, 1282
- The Netherlands, 1272–1273
- United Kingdom, 1252–1253
- Earth observation satellites, 1395–1396
  - CHEOS, 1384–1385
  - commercial remote sensing satellites, 1386–1387
  - environment and disaster monitoring and forecasting, small satellite constellation for, 1385
  - Fengyun, 1383
  - Gaofen, 1385
  - Haiyang, 1384
  - Yaogan, 1385
  - Ziyuan, 1384
- Earth observation security and defense, 706–710
- Earth observation space policy, 411–414
- Ecodesign, 1084
- Economic and financial (E&F) domain, 5
- Economic and financial (E&F) operations, 165
- Economic sovereignty, 223–224
- Economic vulnerability, 748
- Economy, space sector, 1129–1130
- EDA Capability Development Plan, 476, 481
- EDA GOVSATCOM Demonstration Project, 1202
- Effective Space Solutions, 594
- Efficiency-thoroughness-tradeoff, 138
- Egypt-Israel Peace Treaty, 591
- E-health, 636
- EIRSAT-1, 1309
- Electronic intelligence (ELINT)
  - France, 1235–1236
  - satellite, 1159
- Electronic warfare (EW), 926–927
- Electro-optical sensors, 976
- Emergency Mapping Organizations, 753
- Emirates Institution for Advanced Science and Technology (EIAST), 639
- Emirates Space Innovation Group (ESIG), 649
- Enhanced imagery system (EIS), 1151
- Enhanced polar system (EPS), 1146
- Environmental Consequences of Orbital Breakups (ECOB), 858, 859
  - long-term effect, 859
  - mid-term effect, 859
  - short-term effect, 859
- Environmental Control and Life Support Systems (ECLSS), 1434
- Environmental damage, 674–679
- Environmental Mapping and Analysis Program (EnMAP), 1239
- Environmental vulnerability, 750
- Environment and disaster monitoring, 909
- Environment capacity
  - applications, 862–863
  - definition, 859
  - scheduling and monitoring process, 861
- Equatorial Launch Australia (ELA), 1449–1450
- ERNST, 1240
- Eshel, Amir, 592
- Estonia
  - EO, ISR, 1298–1299
  - PNT, 1300
  - SATCOM, 1299–1300
  - space and security budget, 1298
  - SSA, 1300
- EU Global Strategy, 468
- EU Research Framework Programme, 1194
- Euroconsult, 668
- Europe, 362
  - economic and financial (E&F) operations, 171–173
  - space activities in, 21
- European Centre for Medium-Range Weather Forecasts (ECMWF), 431, 435, 443
- European Commission, 1194–1195
- European Cooperation for Space Standardization (ECSS), 1572
- European countries, national space and security/defense strategies, 469
  - France, 469–475
  - Germany, 475–476
  - Italy, 476–478
  - priorities and trends in, 481–482
  - Spain, 478–479
  - United Kingdom, 479–481
- European Defence Action Plan, 726
- European Defence Agency (EDA), 1196–1197
  - activities and programs, 1199–1201
  - and ESA, 1202–1203
- European defense industrial development program (EDIDP), 1196

- European defense research program (EDRP), 1196
- European External Action Service (EEAS), 1195–1196, 1341, 1342
- European Flood Awareness Systems (EFAS), 745
- European Forest Fire Information System (EFFIS), 746
- European Geostationary Navigation Overlay Service (EGNOS), 798, 800, 1204
- European Geostationary Navigation Overlay System, 412
- European Global Navigation Satellite Systems Agency, 641
- European GNSS Agency (GSA), 1204–1205
- European Organisation for the Exploitation of Meteorological Satellites (EUMETSAT), 428, 431, 435, 443, 487
- European Security and Defence Identity (ESDI), 404
- European Security and Defence Policy (ESDP), 402
- European Space Agency (ESA), 6, 246, 249, 250, 257–258, 405, 414, 468, 469, 473, 482, 486, 794, 848, 853, 854, 1006, 1039, 1192, 1201–1203, 1437, 1500, 1572
  - Earth observation, 1208–1210
  - export control regulations, 203–205
  - PNT, 1212–1213
  - SATCOM, 1210–1212
  - space security status, 1207–1208
  - SSA/SST, 1213–1214
- European space and security governance
  - archetype model, 442–445
  - France, 425–427
  - Germany, 427–428
  - Italy, 429–430
  - multilateral level, 431–442
  - Spain, 428–429
  - United Kingdom, 430–431
- European space model, 1504–1508
- European Space Operations Center (EOC), 1341
- European space security policy
  - defense domains, 456–457
  - European autonomy, 453–456
  - European Union role, 457–458
  - intergovernmental model, 460
  - responsibilities, 458
  - risks, 460
  - socio-economic rationale and service-oriented policy, 452
  - space surveillance & tracking, 451
  - space traffic management, 461–463
  - threats, 450
- European Space Surveillance and Tracking Support Framework (EU SST), 885
- Consortium, 888–889
- data policy, 894–895
- data sharing & processing, 894
- European Union space program, 898–899
- evolution as sensor network, 893–894
- interaction with European Union Stakeholders, 891
- internal governance, 889–891
- legal basis, 887–888
- sensor network, 893–894
- service provision model, 892–893
- services, 895–896
- space traffic management, 899–900
- transatlantic relationships, 891–892
- users, 896
- European Telecommunications Satellite Organization (EUTELSAT), 672
- European Union (EU), 362, 468, 1192
  - Earth observation, 1198–1201
  - EDA, 1196–1197
  - EEAS, 1195–1196
  - European Commission, 1194–1195
  - export regulations, 200–203
  - legal basis for space, 1193
  - PNT, 1203–1205
  - PSC, 1195
  - Satcen, 1197–1198
  - SATCOM and cross-domain applications, 1201–1203
  - SATCOM for security, 793–794
  - SSA/SST, 1205–1207
- European Union Military Committee (EUMC), 1195
- European Union Satellite Centre (Satcen), 1197–1198
- European Union Satellite Communication Market (EU SatCom Market), 791, 1202
- Eutelsat satellite, 869
- Evolved Enhanced CRYSTAL System (EESC), 1153
- Evolved strategic system (ESS), 1139
- Experimental Satellite Communication Earth Station (ESCES), 576
- Export Administration Regulation (EAR), 194–197
- Export controls
  - definition, 187
  - ESA, 203–205

- international legal regimes, 189–194
  - national and regional legal regimes, 194–203
- Export restrictions, 6
- Externalities, 1519
  
- F**
- F-15 Eagle airplane, 870
- Federal Space Program, 394
- Fengyun-1C, 1081
- Fengyun satellite series, 908
- Fengyun series satellites, 1383
- Finland
  - EO, ISR, 1302–1303
  - PNT, 1304
  - SATCOM, 1303–1304
  - space and security budget, 1301
  - SSA, 1304–1305
- Fire Bispectral InfraRed Detector (FireBIRD), 1240
- First Korea Space Launch Vehicle (KSLV-1), 1174
- Five Eyes community (FVEY), 442
- Fixed-Satellite Service (FSS), 780, 993, 999
- Flemish Institute for Technological Research, 1269
- Fly Your Satellite (FYS) program, 1309
- Food and Agriculture Organization (FAO), 761
- Food insecurity, 761
- Ford, Gerald, 374, 376
- Forecasting, 909
- Foreign Military Sales (FMS), 1232
- Forensics investigation/analysis, 932
- Foresight methods, 141
- Fractional Orbital Bombardment System (FOBS), 373
- Fragmentation (FG) service, 896
- France, 425–427
  - ELINT, 1235–1236
  - EO, ISR, 1227–1230
  - military satcom, 788
  - PNT, 1232–1233
  - SATCOM, 1230–1232
  - space and security budget, 1227
  - space and security status, 473
  - SSA, 1233–1235
  - strategic documents, space and security elements in, 473–475
- Franco-German Summits and Security and Defence Council (CFADS), 437
- French Law on Space Operations, 1103
- French Space Operations Act, 473, 1067
  
- French space security programs
  - action, 1338–1339
  - co-orbital spatial rendezvous, 1334
  - cyber-attacks, 1334
  - dependency, 1330–1332
  - directed energy weapons, 1333
  - European Union, cooperation within, 1340–1342
  - hard attack, ground segment, 1333
  - high altitude nuclear weapons, 1333
  - jamming, 1333–1334
  - knowledge, 1337–1338
  - modernization, 1339–1340
  - protection, 1338
  - resilience, 1337
  - space surveillance capabilities, 1334–1336
- Frequency allocations, 989
- Frequency-Division Multiple Access techniques, 804
- Frequency management
  - advance publication information (API) procedure, 991
  - allocations, 989
  - BSS plans, 999
  - coordination, 992
  - FSS plan, 1000
  - MIFR, 995
  - non-GSO system, 993
  - non-planned space services, 991
  - notifying administration, 997
  - protection of frequency assignments, 1002
  - regulations, 990, 991
  - short duration mission, 998
- Frontex, 1199
- Functional disaggregation, 133
- Functional resonance analysis method, 139
  
- G**
- Gaganyaan project, 1434, 1435
- Galileo, 1203–1204
  - flagship programme, 1490
  - program, 817
  - satellite navigation system, 1376
  - system, 830
- Gaofen satellite series, 909
- Gaofen series satellites, 1385
- Gavin, James, 371
- Gender equality, 637–638
- General Affairs and External Relations Council (GAERC), 403
- General Armaments Department (GAD), 546



- General Personal Data Protection Act (LGPD), 662
- General Staff Department (GSD), 546
- Generic Military Task List (GMTL), 711
- Geneva Protocol, 190
- Geodynamic Network of the Academy of Sciences (GEONAS), 1294
- Geomagnetic storm, 1009
- Geomagnetosphere, 1035
- Geonavigation, 764–765
- Geospatial Intelligence (GEOINT) communities, 706, 719
- Geostationary Earth orbit (GEO), 573, 783, 942, 1065–1069, 1383
- Geostationary satellite orbit (GSO), 989, 992, 993, 1085, 1086
- Geosynchronous communications satellites, 532
- Geosynchronous equatorial orbit (GEO), 302–303, 307, 310, 314
- Geosynchronous Launch Vehicle (GSLV), 1423, 1425, 1426, 1431, 1432, 1435, 1436
- Geo Synchronous Launch Vehicle Mark III (GSLV MkIII), 1423, 1426, 1431, 1432, 1434, 1435
- Geosynchronous Satellite Launch Vehicle (GSLV), 573, 575
- Geo synchronous satellites (GSAT), 1422
- Geosynchronous transfer orbit (GTO), 1403
- GeoTech Innovation Program, 638
- Geo transfer orbit (GTO), 1425, 1432, 1439
- German Remote Sensing Data Center, 1240
- German Space Operations Centre (GSOC), 1241
- German Space Strategy, 475
- German-US ROSAT space telescope, 248
- Germany, 427–428
  - EO, ISR, 1237–1241
  - military satcom, 789
  - PNT, 1242
  - SATCOM, 1241–1242
  - space and security budget, 1237
  - space and security status, 475
  - SSA, 1242–1243
  - strategic documents, space and security elements in, 475–476
- GhanaSat-1 cubesat, 635
- Gilmour, 1450
- Global facility for disaster reduction and recovery (GFDRR), 734
- Global Flood Awareness System (GloFAS), 745
- Globalization, 387
- Global Monitoring for Environment and Security (GMES) programme, 402
  - See also* Copernicus programme
- Global Navigation Satellite Systems (GNSS), 391, 394, 641, 702, 798, 799, 1009
  - Compass system, 805–806
  - in Europe, 835
  - factors to vulnerability of signals, 822
  - Galileo timing, 816–817
  - GLONASS, 804–805
  - GNSS Galileo and EGNOS Systems, 806–809
  - GPS, 801–804
    - interoperability, 809–811
    - multi-constellation defence GNSS receivers, 833
    - open services, 828
    - operational satellites, 799
    - PNT services, 825–827
    - Professional Mobile Radio, 814–816
    - PRS and Brexit, 817–818
    - regulated and access controlled services, 828
    - security applications, 814–818
    - threats to, 812–814
    - in US, 835
    - vulnerabilities, 812
- Global Operational Meteorological Satellite Detection System (GOMSS), 908
- Global positioning service, 822, 826
- Global Positioning System (GPS), 61, 391, 928, 1232
  - design, 801
  - modernization, 803–804
  - services, 802
- Global space governance, 4, 5
  - arms control agreements, 38
  - arms control treaty, 43–45
  - ASAT weapon system, 42–43
  - competition, 37
  - dual-usable assets, 39–41
  - self-interested members, 39
  - space-based assets, 38
  - space powers, 41–42
- Global War on Terror (GWOT), 378
- Global Wildfire Information System (GWIS), 746
- GNSS Security Accreditation Board (GSAB), 1212
- GomSpace, 1296
- GOMX-4, 1295
- Gorbachev, Mikhail, 376

- Governmental Satellite Communications (GOVSATCOM), 362, 784, 791, 1201
- GovSat-1, 790
- Govsatcom Precursor program, 1211
- GPS-aided GEO augmented navigation (GAGAN), 1422, 1429
- GPS modernization program, 1148
- GPS program evolution, 1148
- GRAB satellite, 1159
- Grand Challenge Program, 1449
- Grand Network Adapted to Space Surveillance (GRAVES), 1233–1235, 1335
- Greece
- EO, ISR, 1305
  - PNT, 1306
  - SATCOM, 1306
  - space and security budget, 1305
  - SSA, 1306–1307
- Green Revolution, 774
- Ground/air terminal program, 1139
- Ground-based ASAT tests, 875
- Ground-based electro-optical deep space surveillance, 976
- Ground-based EW systems, 927
- Ground level events (GLE), 1009
- Group of governmental experts (GGE), 1544, 1547
- Growth domestic product (GDP), 468, 470, 471
- Guiana Space Centre, 1185–1186
- Guidance, navigation and control (GNC), 1197
- Guideline for Orbital Debris Mitigation, 1418
- Gulf War, 85
- H**
- Hague Code of Conduct (HCoC), 191, 192
- Hague International Space Resources Governance Working Group, 353
- Hague Peace Conferences of 1899 and 1907, 82
- Haiyang satellites, 1384
- Hard inputs, 967
- Hard X-ray Modulation Telescope (HXMT), 1393, 1397
- Hayabusa mission, 502
- Heating, ventilation, and air conditioning (HVAC) systems, 254
- Helios program, 409–412
- Hélios satellites, 1228
- Hellenic Presidency, 411–412, 417
- Herzliya Science Center Space Lab, 594
- High-altitude nuclear explosions, 872
- High-altitude platform station (HAPS), 1240
- High Altitude Pseudo Satellites (HAPS), 714, 1070, 1210
- High dimensional model representation (HDMR) methods, 955
- High Level Forum (HLF), 627
- Highly elliptical orbit (HEO), 302, 307
- High-powered microwave weapons, 1333
- High Resolution Optical System (HIROS), 1238
- High throughput satellites (HTS), 1072
- Hindustan Aeronautics Limited (HAL), 573
- HISDESAT, 1250
- HISPASAT, 1250
- Hit-to-kill weapons, 871
- Hope Mars Mission, 647
- HOT, 752
- House-keeping telemetry, 256
- Hubble space telescope, 1153
- Human space flight, 1493
- Human spaceflight safety
- human rating, 292–293
  - risks, 294–297
  - suborbital flight regulatory safety framework, 288–291
  - system safety, 287
- Hungary
- EO, ISR, 1307–1308
  - PNT, 1308
  - SATCOM, 1308
  - space and security budget, 1307
  - SSA, 1308
- Hurricane Weather Net (HWN), 1017
- Hydrazine, 283
- Hydroelectric power plant, 678, 681
- HYPERNETS project, 1299
- Hyper-Spectral Imaging Satellite (HysIS), 582
- Hypothesized knowledge, 964
- Hyten, John E., 585
- I**
- Ikonos, 707
- Ilan Ramon International Space Conference, 595
- Imagery analysis, 709, 715
- Imagery Intelligence (IMINT), 1200
- communities, 713, 714
- Imaging radar satellites, 1154
- India, 363
- space activities in, 20
- Indian ASAT test, 60
- Indian Mini Satellite (IMS-1), 1430

- Indian National Committee for Space Research (INCOSPAR), 572
- Indian National Satellite (INSAT), 576, 1422, 1425, 1428
- Indian Navy, 581
- Indian Regional Navigation Satellite System (IRNSS), 1422
- Indian Regional Navigation System, 583
- Indian Remote Sensing (IRS), 1424, 1425, 1431
- Indian Remote Sensing Satellite system (IRS), 576
- Indian space program, 1423, 1426, 1427
  - expansion phase (2000s), 1425–1426
  - experimental phase (1980s), 1424–1425
  - human spaceflight program, 1433–1435
  - hypersonic air breathing engine, 1438–1439
  - initiation phase (1960–1970s), 1423–1424
  - operational phase (1990s), 1425
  - RLV-TD, 1436–1438
  - space applications, 1426–1428
  - space infrastructure, 1428–1430
  - space transportation system, 1430–1432
  - SSLV, 1435–1436
- Indian Space Research Organization (ISRO), 363, 572, 576, 578, 579, 581, 586, 1422–1426, 1428–1435, 1437, 1439, 1574
- India's space programme
  - ANTRIX, 572, 579
  - ASAT test, 583–586
  - ASLV, 573
  - DRDO, 573
  - GEO, 573
  - GSLV, 573, 575
  - HAL, 573
  - INCOSPAR, 572
  - Indian Earth observation satellites, 577
  - INSAT-1, 576
  - INSAT-2, 576
  - military specific space systems, 581–583
  - MTCR, 575
  - national power, 577–579
  - national security, 579–581
  - PSLV, 573, 575, 579
  - SLV-3, 573
  - SSLV, 576
  - Thumba village, 572
- Inferred knowledge, 964
- Information and communication technology (ICT), 363, 544
  - civil-military integration, 547–549
  - PLA Strategic Support Force, 546–547
- Information assurance (IA), 247, 255, 256, 259
- Information dominance, 536–537
- Information-Gathering Satellite (IGS) program, 558–559
- Informationized local wars, 533
- Information sharing network (ISN), 929
- Ingenio, 1249
- INSAT-4B-S, 876
- Integrated agriculture decision support system,
  - agriculture, postharvest loss reduction, *see* Agriculture, postharvest loss reduction
- Integrity check value (ICV), 255
- Intelligence-Surveillance-Reconnaissance (ISR), 118, 369, 927
  - Austria, 1267
  - Belgium, 1269
  - Czech Republic, 1292–1293
  - Denmark, 1295–1296
  - Estonia, 1298–1299
  - Finland, 1302–1303
  - France, 1227–1230
  - Germany, 1237–1241
  - Greece, 1305
  - Hungary, 1307–1308
  - Ireland, 1309–1310
  - Italy, 1244–1245
  - Luxemburg, 1311–1312
  - Norway, 1276
  - Poland, 1314–1315
  - Portugal, 1318–1319
  - Romania, 1321–1323
  - Spain, 1248–1250
  - Sweden, 1280
  - Switzerland, 1282
  - The Netherlands, 1272–1273
  - United Kingdom, 1252–1253
- Inter-Agency Debris Committee (IADC), 848, 852, 855, 856, 860, 862, 863
- Inter-Agency Debris Coordination Committee (IADC), 63, 69
- Inter-Agency Space Debris Committee (IADC), 1084
- Inter-Agency Space Debris Coordinating Committee (IADC), 307, 520, 918, 1418
  - space debris mitigation guidelines, 566
- InterContinental Ballistic Missiles (ICBMs), 369, 370, 376, 580
- Intergovernmental Panel on Climate Change (IPCC), 1083
- Interim polar system, 1145–1146
- Interministerial Commission of Industrial and Space Policy, 429

- International Academy of Astronautics (IAA), 944
- International Aeronautical Congress, 594
- International Association for Advancement of Space Safety (IAASS), 314
- International Asteroid Warning Network (IAWN), 1029, 1032, 1033
- International Civil Aviation Organization (ICAO), 1020, 1022
- International Code of Conduct for outer space activities, 87, 106–107
- International cooperation, 147
- International Covenant on Civil and Political Rights, 1101
- International Frequency Information Circular (BR IFIC), 991
- International Geophysical Year (IGY) competition, 370
- International humanitarian law, 4
- International Maritime Organization (IMO) Convention, 1082
- International Organization of Space Communications (INTERSPUTNIK), 672
- International organizations, space security, 1130–1131
- International Science Council (ISC), 1561
- International Space Environment Service (ISES), 1021
- International space policies, 604
- International space security, 5–7
- International Space Station (ISS), 574, 1433
- International Telecommunications Satellite Organization (ITSO), 672
- International Telecommunication Union (ITU), 59, 310, 431, 458, 782, 860, 861, 1066, 1067, 1069, 1074, 1077, 1080, 1085–1087, 1101
  - administrative due diligence, 1000, 1001
  - advance publication information, 991, 992
  - BSS plans, 999
  - frequencies and orbits usage, 990, 991
  - frequency allocations, 989, 990
  - frequency assignments, coordination of, 992, 993
  - frequency assignments, protection of, 1002, 1003
  - FSS Plan, 1000
  - harmful interference prevention, 1001, 1002
  - MIFR, 995, 996
  - non-GSO system, 993, 994, 998, 999
  - non-planned space services, 991
  - notifying administration, 997
  - organizational structure, 988
  - principles, 988
  - Radiocommunication Sector (ITU-R), 986, 988
  - Radio Regulations, 987
  - satellite registration procedure, 996
  - Telecommunication Development Sector (ITU-D), 986, 988
  - Telecommunication Standardization Sector (ITU-T), 986, 988
- International Traffic in Arms Regulations (ITAR), 68, 197–200
- Internet of things (IoT), 1070
- Internet service providers (ISP), 1073
- Ionic blasts, 1034
- Ionizing radiation, 294
- Ionosphere, 1009
- Iran, 24
- Iran's space activities, 602
  - air and space strategy, 608–609
  - challenges of implementing space policy plans, 614–615
  - comprehensive document of aerospace development, 607–610
  - comprehensive scientific map, 606–607
  - Fourth Development Plan Act, 611
  - international space policy, 604
  - long term aerospace policies, 609–610
  - national space policy, 604–615
  - space security, 615–617
  - supervisory and regulatory structure, 612–614
  - Vision Plan, 604–606
- Ireland
  - EO, ISR, 1309–1310
  - PNT, 1310
  - SATCOM, 1310
  - space and security budget, 1309
  - SSA, 1311
- Iridium, 831
- Iridium-Cosmos collision, 305
- Irma crisis, 736
- Irma, hurricane, 1017
- Islamic State of Iraq and Syria (ISIS), 378
- Israel, 363
  - space activities in, 24
- Israel's approach, space security and sustainability
  - Amos-6, 594
  - C3IEL, 594
  - combat capabilities, 591
  - Duchifat-1, 594
  - Duchifat-2, 594

- Israel's approach, space security and sustainability (*cont.*)  
 Egypt-Israel Peace Treaty, 591  
 Ilan Ramon Space Conference, 592  
 intelligence capabilities, 591, 592  
 Israeli public's awareness, of space activities and research, 594  
 Israel Space Agency, 594  
 national defense reconnaissance satellites, 593  
 national security, 596  
 national space program, 591  
 Ofeq-1, 592  
 Ramon Foundation, 595  
 SpaceIL, 595  
 SSA, 596  
 task-force, 593  
 UN-COPUOS, 597  
 Venus, 594
- Israel Space Agency, 594, 597
- Italian-Argentine System of Satellites for Emergency Management, 639
- Italian space  
 cyber threats, 1359  
 Earth Observation, 1352–1353  
 European space infrastructure and Italian participation, 1353  
 Fucino Space Centre, 1353–1354  
 governance and aerospace sector, 1347–1349  
 history, 1346–1347  
 launchers, 1349  
 Matera Space Center, 1355  
 origin, 1345  
 policy, priorities and strategy, 1359–1363  
 security, 1356–1357  
 SICRAL Joint Control Center, 1354–1355  
 space economy, 1355–1356  
 space threats, 1357  
 surveillance, 1358–1359  
 telecommunication satellite, 1351–1352
- Italian Space Agency, 429
- Italy, 429–430  
 EO, ISR, 1244–1245  
 military satcom, 789  
 PNT, 1246–1247  
 SATCOM, 1245–1246  
 space and security budget, 1243  
 space and security status, 476–477  
 SSA, 1247–1248  
 strategic documents, space and security elements in, 477–478
- Italy's space agency, 1508
- J**
- Jamming, 812  
 effect, 873  
 of space telecommunications, 879
- Japan, 363  
 space activities in, 19
- Japan Aerospace Exploration Agency (JAXA), 558, 559, 563–569
- Japanese Space Security Policy  
 Code of Conduct, 566–568  
 1969 Diet Resolution, 556–557  
 IGS program, 558–559  
 JAXA, 565–566  
 Kawamura Consultation Group, 560  
 MoD, role of, 563–565  
 regional and global security, 562–563  
 SDF, 557  
 strategic objectives, 560–562
- Japanese Theater Missile Defense System, 565
- Japan-US alliance, 363
- Jilin-1 satellites, 1386, 1388
- Johnson, Lyndon, 373
- Joint Air Power Competence Centre (JAPCC), 1216
- Joint Chief of Staff (JCS), 55
- Joint Intelligence, Surveillance and Reconnaissance (JISR), 1216
- Joint Intelligence, Surveillance and Reconnaissance Service Line (JISR SL), 1215
- Joint Probabilistic Data Association (JPDA), 980, 981
- Juste retour rule, 1505
- K**
- Kapustin Yar, 1184, 1185
- Kazakhstan, economic and financial (E&F) operations, 176
- Kennedy, John F., 372, 373
- Kessler syndrome, 221, 241, 847, 850, 852, 857, 859, 863
- Key performance indicator (KPIs), 628
- Khrunichev State Research and Production Space Center, 1175
- Kinetic energy weapons, 871–872
- Kinetic Kill Vehicle (KKV) missions, 584
- Kirchberg Declaration, 408
- Klein, John J., 52
- L**
- Landsat-1 satellite, 706
- Landsat-7 satellite, 248, 876

- Laser bees, 1033
- Latent knowledge, 964
- Latin America
  - economic and financial (E&F) operations, 169–171
  - space activities in, 25
- LauncherOne, 275
- Launch safety
  - air launch safety, 274–276
  - flight safety risk, 272–274
  - risk for maritime and air transportation, 274
  - site ground safety risk, 271–272
- Laws of war, 75, 82–83
  - distinction, principle of, 83–84
  - military objective, principle of, 84
  - outer space, 85–87
  - proportionality, principle of, 84
- Legal Subcommittee (LSC), 1094
- Liability for Damage Caused by Space Objects (LIAB), 657
- Liberal Democratic Party (LDP), 559, 561
- Liberation Tigers of Tamil Eelam (LTTE), 217
- Life cycle assessment (LCA), 1083
- Limited Test Ban Treaty (LTBT), 190
- Local wars under informationized conditions, 530–531
- Long March (LM) launch vehicles
  - LM-11, 1416
  - LM-2, 1406–1409
  - LM-3, 1410–1413
  - LM-4, 1413–1415
  - LM-5, 1415
  - LM-6, 1416
  - LM-7, 1416
- Long-term sustainability (LTS), 847
  - guidelines, 1064
  - of outer space activities, 1551
- Long-term sustainability (LTS) of outer space
  - activities, UAE space policy
  - international cooperation, capacity-building and awareness, 646–649
  - policy and regulatory framework for space activities, 643–645
  - safety of space operations, 645–646
  - scientific and technical research and development, 649–650
- Low earth orbit (LEO), 6, 52, 303–304, 309–312, 314, 783, 847, 848, 852, 867, 942, 947, 949, 1065, 1069, 1072, 1403, 1425, 1435, 1436
- Low energy lasers, 1333
- Lunar Roving Vehicle (LRV), 1014
- Luxembourg
  - EO, ISR, 1311–1312
  - military SATCOM, 790
  - PNT, 1313
  - SATCOM, 1312–1313
  - space and security budget, 1311
  - SSA, 1313
  - use of space resources, 351
- LuxGovSat, 790
- M**
- Maastricht Treaty, 402, 404
- Machine learning (ML), 724
- Magna Carta, 655
- Magnetic reconnection, 1007
- Magnetospheric multiscale (MMS)
  - constellation, 1039
- Managed detection and response support (MDRS), 931, 932
- Managed threat detection (MTD), 931
- Manned Orbiting Laboratory (MOL)
  - program, 373
- Man-related security threats, 1514
- Maritime signals intelligence satellites, 1161
- Mars Orbiter Mission (MOM), 574, 577, 1426, 1429
- Masat-1, 1307
- Mass extinctions, 1026
- Master control station (MCS), 1150
- Master International Frequency Register (MIFR)
  - notification and recording, 995, 996
  - notifying administration, 997
- Matera Laser Ranging Observatory (MLRO), 1247
- Matera Space Center, 1355
- M-code signal, 832
- Meaconing, 813
- Medium-earth orbit (MEO), 307, 783, 828, 1065, 1069, 1072
- Mektory Space Centre, 1299
- Microsatellite (Microsat), 1430
- Microsat-R satellite, 583, 868
- Midcourse Space Experiment (MSX), 976
- Middle East, 23
  - economic and financial (E&F) operations, 175
- Military astronautics, 537
- Military-Industrial Commission, 391
- Military organization model, 55
- Military SATCOM (MILSATCOM), 784, 1273

- Military space operations  
 active defense, 534  
 all aspects unified, 534–535  
 defensive space operations, 542–543  
 key point is space dominance, 535–536  
 space blockades, 540  
 space deterrence, 538–539  
 space information support operations, 543–544  
 space strike operations, 540–542
- Millennium Development Goals (MDGs), 760
- Milstar satellites, 1139
- Miniature homing vehicle (MHV), 870
- Mining activities, 679, 683–685
- Minister for Education, Culture, Sports, Science, and Technology (MEXT), 559
- Ministry for Economic Affairs and Energy, 426, 428
- Ministry of Defense (MoD), 427, 430, 443, 563–565
- Ministry of Finance (MOF), 521
- Ministry of Foreign Affairs (MoFA), 561
- Ministry of Industry and Information Technology (MIIT), 522
- Ministry of Transport and Digital Infrastructure, 427
- Missile early warning satellites, 1155–1158
- Missile Technology Control Regime (MTCR), 190, 192, 195, 197, 202, 575, 658
- Missile warning systems, 1012, 1013
- Mission Shakti, 583
- MISTY satellite, 1153
- MiTEx satellites, 1166
- Mobile satellite services (MSS), 780
- Mobile user objective system (MUOS) satellites, 787, 1140–1143
- Modi, Narendra, 586
- Modular decomposition, 133
- Mohammed Bin Rashid Space Center, 639
- Molniya orbit, 1145
- Monge A601*, 1234
- Monostatic Space Surveillance Radar (MSSR), 1251
- Moon Agreement (MA), 98, 1081, 1566–1567
- Moriba Jah Refrigerator Approach, 966
- Multiannual financial framework period (MFF), 453
- Multi-domain disaggregation, 133
- Multi-Domain Operations (MDO), 1218
- Multinational Geospatial Support Group (GSG), 1217
- Multinational space-based imaging system (MUSIS), 1229
- Multi-orbit disaggregation, 133
- Mutual assured destruction (MAD), 376, 718
- N**
- NASA EOS AM–1 satellite, 248
- NASA International Internship Program, 648
- National Academies of Science (NAS), 68
- National Advanced Optical System (NAOS) Program, 1269, 1311
- National Aeronautics and Space Administration (NASA), 51, 349, 572, 1029, 1032, 1039, 1437
- National Centre for Space Research (CNES), 425, 426, 441
- National Defense Authorization Act (NDAA), 379
- National Defense Mobilization Law, 519
- National Defense Program Guideline, 569
- National Defense Strategy (NDS), 56, 57
- National Institute for Space Activities (INPE), 657
- National Oceanic and Atmospheric Administration (NOAA), 1017, 1021, 1022, 1036
- National People’s Congress (NPC), 519, 522
- National Radio Administration Bureau, 523
- National Radio Management Plan, 522
- National security, 922
- National Security Space Strategy (NSSS), 58, 477
- National Security Strategy (NSS), 56, 361, 368, 381
- National Space Framework, 625
- National Space Investment Promotion Plan, 646
- National Space law, 625, 1067
- National Space Policy (NSP), 368, 380, 382
- National Space Science and Technology Centre (NSSTC), 628
- National Space Strategy (NSSS), 368, 378, 380, 381
- National Space Strategy, 625
- National space traffic management policy, 461
- National Strategy for Space, 56, 57
- NATO Communication and Information Agency (NCIA), 1218
- NATO SATCOM Post-2000 (NSP2K) program, 792, 1218
- NATO Support and Procurement Agency (NSPA), 1216

- Natural language processing (NLP), 968  
 Natural monopolies, 1518  
 Natural resources, exploitation and pillage of, 679–685  
 Nature-related security threats, 1514  
 NavHub system, 1242  
 Navigation Innovation and Support Programme (NAVISP), 1212  
 Navigation satellite systems, China, 912  
 Navigation with Indian Constellation (NaVIC), 1429  
 NAVWAR (Navigation Warfare), 802, 813, 825  
 Near-Earth objects (NEO), 70, 1032, 1214  
 Near-Earth space, 623  
 Nearest Neighbor (NN) approach, 980  
 Netherlands Positioning Service (NETPOS), 1274  
 New Space, 1474  
 New space economy  
   description, 1500  
   European space model, 1504–1508  
   transformation of space security, 1502–1504  
   US space policy, 1500–1502  
 NewSpace program, 638  
 Nixon, Richard, 372, 374  
 No First Placement of Weapons in Outer Space (NFP), 1545  
 Non-geostationary orbit (NGSO), 783  
 Normal accident theory (NAT), 135  
 North American Aerospace Defense Command (NORAD), 1334  
 North America, space activities in, 26  
 North Atlantic Treaty Organization (NATO), 118, 220, 792, 1192  
   bombing campaign, 86  
   defense expenditure, 471  
   Earth observation/intelligence, surveillance and reconnaissance, 1216–1217  
   PNT, 1219  
   SATCOM, 1218–1219  
   space and security status, 1215–1216  
   SSA/SST, 1220  
 Norway  
   EO, ISR, 1276  
   PNT, 1277–1278  
   SATCOM, 1276–1277  
   space and security budget, 1275–1276  
   SSA, 1278–1279  
 Norwegian CryoClim project, 1276  
 Norwegian Space Centre (NSC), 426  
 NovaSAR-S, 1253  
 NovaSAR small synthetic aperture radar satellite, 1375  
 Nuclear detonation detection system (NDS), 1158  
 Nuclear Non-Proliferation Treaty (NPT), 190  
 Nuclear Suppliers Group (NSG), 190
- O**  
 Obama, Barack, 378, 380  
 Oberg, James, 51  
 Ocean satellite series, 908  
 Office of Foreign Asset Control (OFAC) Regulations, 195  
 OneWeb constellation, 854  
 On-orbit services (OOS), 214  
 Onsala Space Observatory (OSO), 1281  
 Open procurement, 1372  
 Open Street Map, 748  
 Operational Center for Military Surveillance of Space Objects (COSMOS), 1335  
 Operational linescan system, 1162  
 Operation Anaconda, 1015  
 Optical and Radar Federated Earth Observation system (ORFEO), 1228  
 Optical imaging satellites, 1151–1154  
 OPTSAT-3000, 1245, 1352  
 Orbital debris, 276–277  
   collision risk with, 277–279  
   remediation, 280–282  
   risk control, 279–280  
 Orbital rescue, 296–297  
 Orbit determination (OD), 977–980  
 Ore processing, 684, 685  
 Organizational structures, 54–56, 61, 67  
 Other celestial bodies (OST), 655  
 OTOS program, 1229  
 Outer space, 192–194  
   arms control in, 99–102  
   domestic arms control, 107  
   International Code of Conduct for, 106–107  
   laws of war, 85–87  
   military uses of, 80–82  
   multilateral treaties, 79  
   non-appropriation principle, 76–78  
   space-related principles, 79–80  
   treaty, 96–98  
   UNCOPUOS, 76  
   use of force against, 102–106  
 Outer Space Act 1986, 479  
 Outer space security  
   aerospace and defence sector, 1521–1527  
   commercial considerations, 1528  
   economic activity and society, 1527–1528



- Outer space security (*cont.*)  
 geopolitical dynamics and partnerships, 1512  
 hardware/space assets and weaponization, 1512  
 political economy, 1529–1531  
 security dimensions and challenges, 1513–1515  
 space industry, 1515–1519  
 sustainability, 1512
- Outer Space Treaty (OST), 43, 52, 54, 59, 62, 65–67, 77–81, 90, 146, 212–214, 373, 374, 586, 1064, 1068, 1075, 1076, 1094, 1096, 1097, 1118, 1565  
 of 1967, 4, 623, 643, 645  
 Article I, 78, 350  
 Article II, 77, 78, 350  
 Article III, 350  
 Article IV, 81
- Ozone monitoring instrument (OMI), 1273
- P**
- Pact of Paris, 82
- Pad abort test, 1422, 1433
- Pakistan  
 challenges, 1457, 1468  
 international cooperation, 1466–1467  
 Pakistan Remote Sensing Satellite (PRSS)-1, 1456  
 Pakistan's National Space Agency, 1456–1457  
 Pakistan's Space Vision 2047, 1467–1468  
 Pakistan Technology Evaluation Satellite (PakTES)-1A, 1456  
 socioeconomic benefits, 1464–1466  
 space activities in, 21  
 Space and Upper Atmosphere Research Commission (SUPARCO), 1456, 1458  
 space educational institutions, 1460–1461
- Partial Test Ban Treaty, 99
- Passivation, 280
- People's Liberation Army (PLA), 363, 528  
 new historic missions, 530
- Performance variability, 138
- Permanent Structured Cooperation (PESCO), 1196
- Persian Gulf War, 407
- Personally identifiable information (PII), 772
- PHAROS, 1229
- Phased-array radars, 976
- Phobos, 1576
- Physical vulnerability, 748
- Piero Fanti Space Centre, 1353–1354
- Placement of Weapons in Outer Space (PPWT) Treaty, 45
- Planetary Protection Policy (PPP)  
 diplomatic community, initial activities of, 1562  
 initial scientific policies, 1562  
 international law, 1565  
 legal policies, 1562–1563  
 MA and elaboration of legal regulation, 1566–1567  
 revisions to PQR, 1565–1566  
 scientific regulation, PQR, 1563–1564  
 transformation of PQR, 1567
- Planetary quarantine requirements (PQR)  
 revisions to, 1565–1566  
 scientific regulation, 1563–1564  
 transformation of, 1567
- PLA Strategic Support Force (PLASSF), 363, 546–547
- Pléiades High Resolution (PHR), 1228
- Pléiades satellites, 1228
- Plesetsk Cosmodrome, 1182–1183
- PNOTS, 1248, 1249
- Poland  
 bilateral cooperation, 492–493  
 Department of Defense Projects, 488  
 EO, ISR, 1314–1315  
 ESA and, 496–497  
 European Union SST Consortium and role of, 493–495  
 in international programs, 488  
 Military Satellite Technologies Department, 487  
 multilateral programs, 492–497  
 national programs, 490–491  
 PNT, 1316  
 SATCOM, 1315–1316  
 security and defense strategy, 487–489  
 space and security budget, 1313  
 space law and space strategy, 489–490  
 SSA, 1316–1317
- Polar lights, 1010
- Polar Satellite Launch Vehicle (PSLV), 573, 575, 579, 1423, 1425, 1426, 1430–1432, 1435, 1436
- Polish Space Agency (POLSA), 486–487
- Political and Security Committee (PSC), 1195
- Portugal  
 EO, ISR, 1318–1319  
 PNT, 1320  
 SATCOM, 1319–1320  
 space and security budget, 1317–1318  
 SSA, 1320–1321

- Positioning, navigation and timing (PNT), 927,  
1203–1205, 1212–1213, 1219
- Austria, 1268
  - Belgium, 1270–1271
  - Czech Republic, 1293–1294
  - Denmark, 1297
  - Estonia, 1300
  - Finland, 1304
  - France, 1232–1233
  - Germany, 1242
  - Greece, 1306
  - Hungary, 1308
  - Ireland, 1310
  - Italy, 1246–1247
  - Luxemburg, 1313
  - Norway, 1277–1278
  - Poland, 1316
  - Portugal, 1320
  - Romania, 1324
  - Spain, 1251
  - Sweden, 1280–1281
  - Switzerland, 1283–1284
  - The Netherlands, 1274–1275
  - United Kingdom, 1255–1256
- Position, Navigation and Timing (PNT) service,  
702, 704
- GNSS services and systems, 825–829
  - history, 823–825
  - hybrid and autonomous systems, 837
  - impacts on military task, 838–841
  - modernization, 832, 833
  - multi-constellation defence GNSS  
receivers, 833, 835
- Post-harvest food loss (PHL), 760
- Postharvest loss optimized integrated decision  
support system (POIDS), 773
- Post-mission disposal (PMD) rule, 855, 859
- Post-processing Positioning Services  
(PPS), 830
- Potentially hazardous asteroids, 1026–1030
- PRESAGO project, 1246
- Prevention of an Arms Race in Outer Space  
(PAROS), 63, 100, 335, 664, 1541
- Prevention of Placement of Weapons in Outer  
Space Treaty (PPWT), 41, 63, 1544
- PRISMA mission, 1244
- Private finance initiative (PFI), 564
- PROBA2 Science Centre (P2SC), 1271
- Progress Rocket Space Center, 1175, 1176
- Project Oberon, 1375
- Project Team Space-Based Earth Observation  
(PT SBEO), 1200
- Proliferation, 117
- Protected regions, 852
- Protection, 117
- Proton-M, 1175
- PSSI Global Map, 166
- Public and private property, destruction of,  
682–688
- Public goods, 1518
- Public health, 636
- Public private partnership (PPP), 258
- Public regulated service (PRS), 815,  
817–818, 1503
- Purple Mountain Observatory (PMO) in  
Nanjing, 915
- Putin, Vladimir, 386, 389, 392, 395
- Q**
- Quantum communication infrastructure  
(QCI), 1194
- Quantum Experiments at Space Scale  
(QUESS), 1393–1394, 1397
- QUASAR satellites, 1145
- Quasi-territorial jurisdiction, 213
- R**
- Radar Imagery Applications Supporting  
Actionable Intelligence (REACT), 1200
- Radio frequency, 516, 521–523
- Radio navigation-satellite service  
(RNSS), 1001
- Radio Regulations Board (RRB), 988
- Radio Regulations (RR) treaty, 782
- Radio-thermal generators, 284
- RAIM-receiver autonomous integrity  
monitoring, 799
- Ramon Foundation, 595
- RapidEye mission, 1240
- RASOR project, 748
- Reagan, Ronald, 375
- Reconstitution, 117
- Recovery observatory effort, 754–756
- Re-entry (RE) service, 895
- Register Convention, 1066, 1067
- Registration, Evaluation, Authorization and  
Restriction of Chemicals (REACH)  
regulation, 1083
- Remotely piloted aircraft (RPA), 1219
- Remotely piloted aircraft systems (RPAS),  
714, 1211
- Remote sensing, 764
- satellite, 87

- Remote sensing data, security exceptions
  - international level, 1093–1102
  - national level, 1103–1109
  - regional level, 1109–1118
- Renewed Anti-satellite (ASAT), 500
- Rescue Agreement, 1083
- Research and development (R&D), 629
- Resident space objects (RSOs), 306, 951, 967
- Resilience, 5, 116, 117, 128, 230, 1337
  - analysis grid, 139
  - architecture and infrastructure, 132–135
  - capability-resilience trade-off, 134
  - critical infrastructure protection and non-dependence, 131–132
  - deterrence in threat environment, 129–130
  - foresight, 141
  - functional elements of, 133–134
  - operations and organizations, 132–135
  - performance variability, 138
  - practical measures, 134, 138–139
  - principles of, 237–239
  - quality of functional architecture, 132–133
  - sense-making, 136–138
  - in space security policy, 129–132
  - space situational awareness, 140
  - transparency measures and partnerships, 140–141
- Restricted Service (RS), 583
- Restriction of Hazardous Substances (RoHS), 1083
- Reusable Launch Vehicle–Technology Demonstrations (RLV-TD), 1436–1438
- Revolution in Military Affairs (RMA), 581
- R-7 Intercontinental Ballistic Missile, 1172
- RISAT I, 582
- RISAT II, 582
- Rocket technology, 1502
- Rocket, 1178–1179
- Romania
  - EO, ISR, 1322–1323
  - PNT, 1324
  - SATCOM, 1323
  - space and security budget, 1321
  - SSA, 1324
- ROSAT, 876
- Ross, Wilbur, 1065
- Rosse Solar-Terrestrial Observatory (RSTO), 1311
- Route optimization, 766
- Royal Netherlands Air Force (RNAF), 1274
- Royal Observatory of Belgium (ROB), 1270
- Rumsfeld, Donald, 377
- Russia, 361
  - economic and financial (E&F) operations, 178
  - military SATCOM, 792
  - space activities in, 28
- Russian Federation, 386
- Russian GLONASS system, 804–805
- Russian Space Forces, 394
- Russian space launch program, 1183–1184
  - Angara, 1174
  - Baikonur Cosmodrome, 1181–1182
  - Dnepr, 1180
  - Guiana Space Center, 1185–1186
  - Kapustin Yar, 1184, 1185
  - Plesetsk Cosmodrome, 1182–1183
  - Proton-M, 1175
  - Rocket, 1178–1179
  - Sea Launch, 1186–1187
  - Soyuz-2, 1175–1176
  - Soyuz-FG, 1176–1177
  - Strela, 1177–1178
  - Yasny Cosmodrome, 1185
- Russia's space security policy, 393–395
  - ASATs, 389
  - period of retrenchment, decline and dependency, 390–391
  - Russia-Georgia Conflict, 392–393
  - securitization and militarization of space, 391–392
  - space diplomacy, 395–397
- S**
- San Marco 1, 1346
- Sarabhai, Vikram, 573
- SARah system, 1238
- Sardinia Radio Telescope (SRT), 1247
- SAR-Lupe program, 1237
- SATAM, 1234
- SatCen, 723, 724, 728
- Satcom, 702
- SatComBw-Stage 2 program, 789
- Satellite-based Earth observation
  - Copernicus emergency management service (*see* Copernicus emergency management service)
  - missions, 750
  - risk and risk mitigation, 746–750
- Satellite-Based Modular Warning System, 1241
- Satellite communication (SATCOM), 1201–1203, 1210–1212, 1217–1219
  - Austria, 1267–1268
  - Belgium, 1269–1270
  - Czech Republic, 1293

- Denmark, 1296–1297
- Estonia, 1299–1300
- Finland, 1303–1304
- France, 1230–1232
- frequency bands and orbits, 782–783
- Germany, 1241–1242
- Greece, 1305–1306
- historical evolution, 780–781
- Hungary, 1308
- Ireland, 1310
- Italy, 1245–1246
- Luxemburg, 1312–1313
- for military, 784–793
- Norway, 1276–1277
- outlook and perspectives, 795
- Poland, 1315–1316
- Portugal, 1319–1320
- Romania, 1323
- for security, 793–795
- Spain, 1250–1251
- Sweden, 1280
- Switzerland, 1282–1283
- The Netherlands, 1273–1274
- United Kingdom, 1253–1255
- Satellite Data Security Act (SDSA), 1109
  - national security restrictions, 1105–1107
  - and regional context, 1108–1109
  - scope of, 1104–1105
- Satellite Industry Association, 186
- Satellite Instructional Television Experiment (SITE), 1424
- Satellite Launch Vehicle-3 (SLV-3), 573
- Satellite navigation, 1490
  - China, 912
- Satellite remote sensing information, 702
- Satellites services, protection of, 1072–1075
- Satellite Telecommunication Experimental Project (STEP), 1424
- Satellite Time and Location (STL) service, 831
- Scanning Imaging Absorption Spectrometer for Atmospheric Cartography, 1272
- Science, Technology and Industry for National Defense (SASTIND), 549
- Science and Technology Agency (STA), 556
- ScyLight, 1211–1212
- Sea Launch, 1186–1187
- Search-and-rescue (SAR) system, 294
- Second-generation BeiDou system (BDS-2), 1390
- Second World War, 83
- Secure Satcom for Safety & Security (4S), 1210
- Security definition, 12
- Security module, 818
- See Traffic Management (SeeTM) system, 949
- Selective Availability anti-Spoof Module (SAASM), 827
- Self-Defense Forces (SDF), 557, 562–565, 568
- SensorSat, 1165
- SENSUM project, 750
- Sentinel and safeguard program, 870
- Shenzhou-1, 516
- Shenzhou-5, 516
- Shenzhou-8, 516
- Shijian-13 (Chinasat-16) satellite, 1389
- Shijian series, 1391
- Short duration mission (SDM), 998
- Shuttle program, 295
- SICRAL 1, 1246
- SICRAL 1A, 789
- SICRAL 2, 441, 789, 790, 1246
- SICRAL Joint Control Center, 1354–1355
- SIGINT Seniors Europe (SSEUR), 442
- Signals Intelligence (SIGINT), 442
- Sino-French Joint Commission on Space Cooperation, 1398
- Sirio, 1346
- Situational awareness in space (SSA), 927
- Situation Awareness Behaviorally Anchored Rating Scale (SABARS) approach, 938
- Situation Awareness Global Assessment Technique (SAGAT), 938
- Skynet system, 564, 1373
- Skynet 5, 788
- Small and medium enterprises (SMEs), 258
- Small Business Exploratory Research Program, 1449
- Small Satellite Launch Vehicle (SSLV), 576, 1435–1436
- SmartSat CRC, 1451
- Social vulnerability, 748
- Socioeconomic Data and Applications Center (SEDAC), 1051
- Soft inputs, 967
- Solar corona, 1007, 1019
- Solar flares, 1007, 1017, 1028, 1035
- Solar storm, 1029, 1034, 1036
- Sounding Rocket Vehicles (SRV), 603
- South and Southeast Asia, economic and financial (E&F) operations, 175–176
- Southern Launch, 1450
- South Korea, space activities in, 21
- Sovereignty
  - economic sovereignty, 223–224
  - and jurisdiction, 212–214
  - State sovereignty and homeland security, 215–217

- Sovereignty (*cont.*)
- State sovereignty and military domain, 218–220
    - vertical territorial sovereignty, 221–223
- Soviet ASAT, 374
- Soyuz-2, 1175–1176
- Soyuz-FG, 1176–1177
- Space and cyber threats
- astro-hackers, 247–249
  - end-to-end cybersecurity, 254–255
  - equipment destruction/theft, 254
  - identification and assessment of risks, 252
  - identification and assessment of vulnerabilities, 252
  - mission categories and security profiles, 259–262
  - motivations of attackers, 250–251
  - payload data, 256
  - tele commands, 255
  - telemetry, 255–256
  - unauthorized operation of satellite/launcher/spacecraft/ground facilities, 253
  - unavailability of critical services, 254
- Space avoidance, 117
- Space-based assets, 38
- Space-based Earth Observation (SBEO)
- applications, 713–717
  - Copernicus SEA, 719–723
  - EU SatCen, 724–728
  - missions and applications, 710–713
  - monitoring of military installations, 718
  - operational tasks, 717–719
  - treaty verification, 718
- Space-Based Infrared System (SBIRS), 1158
- Space-based space surveillance, 1164–1165
- Spaceborne Hyperspectral Applicative Land and Ocean Mission (SHALOM), 1245
- Space capabilities, 531–533
- Space Certification Body (SCB), 660–661
- Space Climate Observatory (SCO), 672
- Spacecraft platform control, 1144
- Space Data Association (SDA), 306
- Space data systems (SDS), 1145
- Space debris, 80, 88, 304–305, 316, 942
- Space Debris Action Plan, 918
- Space debris mitigation, 846–848, 850, 852, 853, 855–857, 860–863, 1087–1088
- China, measures in, 520–521
  - guidelines, 1083
  - ITU, 1085–1087
  - regulation of space debris, outer space and maritime for, 1082–1083
  - sustainable development, 1083–1084
- Space Defense Initiative (SDI), 376
- Space deterrence, 113, 538–539
- adversary's decision making, primacy of, 119–120
  - credibility and political will, 120–121
  - denial, 116–119
  - effective communication, 121–122
  - escalation, 122
  - punishment, 114–116
  - strategic misperception, 122–124
  - terrestrial aspect, 124
- Space domain, 926, 963
- Space domain awareness (SDA), 962, 964
- calibration, 969
  - defined, 963
  - human-based (soft inputs), 967–968
  - independent observations and Big Data, 969–970
  - metadata, 969
  - purpose, 963, 964
  - standards, 968
  - structured and unstructured information, 968
- Space domain events and processes, 965
- Space domain information fusion (SDIF)
- model, 970–975
- Space domain mission assurance, 132
- Space dominance, 537
- Space economy, 231
- definition, 1473
  - GBORD for selected countries, 1478–1481
  - government R&D priorities, 1480
  - government space expenditure, 1475
  - historical and forecast for civil government space expenditures, 1494–1495
  - Luxembourg and USA budgets, 1478
  - simplified value chain, 1474
  - space budgets, civil and defence, 1477–1479
  - worldwide national space budgets, 1475
- Space environment, 848–854
- Space environment protection and preservation (SEPP), 454
- Space export control law and regulations, *see* Export controls
- Space fence, 277
- Space Force Acquisition Council (SFAC), 56
- Space Force Act, 55
- Space governance, 4
- SpaceIL, 595
- Space information support operations, 543–544

- Space infrastructure
  - components, 232
  - vs. critical space infrastructure, 233–234
  - definition, 231
- Space infrastructure security (SIS), 454
- Space law, general principles of, 75–80
- Space mission assurance, 116
- Space Mission Planning Advisory Group (SMPAG), 1033, 1034
- Space object tracking, 977–983
- Space operations
  - in GEO, 1065–1069
  - in LEO, MEO and transit orbits, 1069–1072
- SpacePharma, 594
- Space Policy Directives (SPDs), 368
  - SPD-1, 382
  - SPD-2, 382
  - SPD-3, 382
  - SPD-4, 383
- Spacepower, 1367–1368
- Spacepower theory, 4, 51, 53, 65, 67, 68
  - environmental sustainability and survival, 69–70
  - goal of, 50
  - hard power and sustainable security, 58–65
  - Oberg, James, 51
  - and US space policy, 57–58
- Space program(s)
  - history of, 1126
  - Soviet Union's, 1126
- Space program in US military and intelligence agency, 1135
  - advanced extremely high frequency satellites, 1138–1139
  - cost, 1135
  - global positioning system, 1147–1151
  - GSSAP, 1165–1168
  - interim polar system, 1145–1146
  - maritime signals intelligence satellites, 1161
  - Milstar satellites, 1139
  - MUOS and UFO, 1140–1143
  - nuclear detonation detection system, 1158
  - relay satellites, 1144–1145
  - signals intelligence satellites, 1159–1161
  - space-based space surveillance, 1164–1165
  - surveillance, 1151–1164
  - telecoms, 1136–1146
  - weather satellites, 1162–1164
  - wideband global satcom, 1143–1144
- Space safety
  - acceptable safety levels, 269–270
  - definition, 266
  - fields, 266–268
  - human spaceflight, 287–297
  - launch safety, 271–276
  - on-orbit safety (*see* Orbital debris)
  - reentry safety risk, 282–286
  - regulations and standards, 286–287
  - safety rules and compliance verification, 270–271
- Space Safety Programme (S2P), 1213
- Space security, 4, 320–321, 1064, 1536
  - Arms Control, 1541
  - capabilities, 502
  - Counterspace Capabilities, 1546
  - definition of, 11–16
  - dynamics, 501
  - evolution, 13–15
  - GEO, space operations in, 1065–1069
  - global governance aspects, 510
  - governance and theoretical perspectives, 4
  - India, 506
  - LEO, MEO and transit orbits, space operations in, 1069–1072
  - military operations, 503
  - military technologies, 507–509
  - moon missions, 502
  - PLA Strategic Support Force, 505–506
  - private sector commercial players, 500–501
  - Russia's institutional innovation, 506
  - satellites services, protection of, 1072–1075
  - spacefaring powers, 509
  - Space Safety, 1536
  - Space Situational Awareness, 510–511
  - Space Sustainability, 1536, 1551
  - space weaponization, 1537
  - specialised institutions, 503–504
  - US Space Force, 504
- Space Security Index (SSI), 15
- Space Security Programs
  - Australia, 1129
  - Britain, 1128
  - China, 1128
  - Europe, 1127
  - France, 1128
  - India, 1128
  - Italy, 1128
  - Russia, 1127
  - United States (US), 1126
- Space situational awareness (SSA), 59–62, 115, 140, 247, 306–307, 314–315, 362, 380, 454, 474, 477, 564, 565, 596, 662–664, 702, 703, 891, 894, 898, 899, 944, 946, 951, 955, 1069, 1071, 1072, 1205–1207, 1213–1214, 1219–1220, 1337, 1374
- Austria, 1268

- Space situational awareness (SSA) (*cont.*)
- Belgium, 1271
  - China, 914
  - Czech Republic, 1294
  - Denmark, 1297–1298
  - Estonia, 1300
  - Finland, 1304–1305
  - France, 1233–1235
  - Germany, 1242–1243
  - Greece, 1306–1307
  - Hungary, 1308
  - Ireland, 1311
  - Italy, 1247–1248
  - Luxemburg, 1313
  - Norway, 1278–1279
  - Poland, 1316–1317
  - Portugal, 1320–1321
  - Romania, 1324
  - Spain, 1251–1252
  - Sweden, 1281
  - Switzerland, 1284
  - The Netherlands, 1275
  - United Kingdom, 1256
- Space Situational Awareness System (SSA), 489
- Space strike operations, 540–542
- Space surveillance, role, 975
- Space surveillance and tracking program (SST), 451, 480, 703, 1205–1207, 1213–1214, 1219–1220, 1341, 1503
- Space Surveillance Network (SSN) sensors, 976–977
- Space sustainability, 6, 321
- arms race prevention, 337–338
  - Conference on Disarmament, 334
  - and COPUOS, 325–331
  - EU proposal for International Code of Conduct, 336–337
  - guidelines, 331–333
  - implementation and updating of guidelines, 334
  - international cooperation, capacity-building and awareness, 333
  - multilateral initiatives, 336–338
  - policy and regulatory framework for, 332–333
  - rating, 863
  - safety of space operations, 333
  - scientific and technical research and development, 333
  - transparency and confidence building measures in outer space activities, 335–336
  - and United Nations, 322–325
- Space systems, 228, 238
- Space systems and security, 214–215
- economic sovereignty, 223–224
  - State sovereignty and homeland security, 215–217
  - State sovereignty and military domain, 218–220
  - vertical territorial sovereignty, 221–223
- Space technology, 187, 188
- agriculture, postharvest loss reduction (*see* Agriculture, postharvest loss reduction)
- Space traffic management (STM), 6, 454, 461–463, 848, 899–900, 944–946, 948, 950, 951, 953–957, 1071, 1072
- active debris removal, 314
  - CSTM, 315
  - definition, 846
  - environmental effects, 312
  - environment capacity, 857–863
  - GEO protected region, 302–303
  - large LEO constellations, 309–312
  - LEO protected region, 303–304
  - reentry disposal of satellites, 313
  - space debris, 304–305
  - space situational awareness, 306–307, 314–315
- Space warfare, 529
- Space weather, 1035, 1036
- defense challenges, 1022, 1023
  - historical events, 1009–1018
  - research & observation challenge, 1018, 1019
  - societal challenge, 1019, 1021
  - Sun's impacts, 1007–1009
- Space White Paper, 517
- SpaceX StarLink, 309, 1045, 1135
- Spain, 428–429
- EO, ISR, 1248–1250
  - military satcom, 790
  - PNT, 1251
  - SATCOM, 1250–1251
  - space and security budget, 1248
  - space and security status, 478
  - SSA, 1251–1252
  - strategic documents, space and security elements in, 478–479
- SPAINSAT, 790, 1250
- SPAINSAT-NG, 790
- Special Committee on Space Development (SCSD), 560
- SPIRALE program, 1236

- SPOT-1, 707  
 SPOT 6, 672, 673  
 SPOT-7, 671  
 SPOT satellite, 407, 1228  
 Sputnik-1, 74–76, 370, 780  
 SSA Space Weather Coordination Centre, 1271  
 Standard Positioning Service (SPS), 583  
 Starwars, 873  
 State Administration of Science, Technology and Industry for National Defense (SASTIND), 520, 524  
 State Radio Monitoring Center (SRMC), 523  
 State sovereignty, 218
  - defense domain, peaceful use in, 219
  - economic sovereignty, 223–224
  - and homeland security, 215–217
  - military activities in space, 218–219
  - new regulations and space policy directives, 220
  - vertical territorial sovereignty, 221–223
 STEM/STEAM education, 637  
 STEREO III, 1269  
 STM1, 703  
 Strategic Air Command (SAC), 370  
 Strategic Arms Limitation Talks II Treaty (SALT II), 100  
 Strategic Arms Reduction Talks (START), 376  
 Strategic defense initiative (SDI), 873  
 Strategic deterrence, 122  
 Strategic Headquarters of Space Policy (SHSP), 561  
 Strategic Priority Program on Space Science, 1392  
 Stratolaunch Systems, 275  
 Strela, 1177–1178  
 Stricto sensu, 870  
 Suborbital flight, 288  
 Sunspot index, 1007, 1013  
 Sun synchronous polar orbit (SSPO), 1425  
 SuperView-1, 1387  
 Support vector machine (SVM), 951  
 Surface-to-air missiles (SAMs), 370  
 Sustainable development, 321  
 Sustainable development goals (SDGs), UAE
  - space sector, 760, 761
    - businesses and jobs opportunities, 635
    - clean water and sanitation, 638
    - climate action, 640–641
    - climate and environment, monitoring of, 634–635
    - communication satellites, 634
    - emergency and aid plans and responses, 636
    - gender equality, 637–638
    - health and well-being, 636–637
    - industry, innovation and infrastructure, 638–639
    - land cover and land use mapping, 641
    - logistics management, 635
    - optimized agriculture, 635–636
    - partnerships, 641–642
    - quality education, 637
    - resources management, 636
    - responsible consumption and production, 640
    - space science and technologies, 641
    - sustainable cities and communities, 639–640
    - work and economic growth, 638
 Sweden
  - EO, ISR, 1280
  - PNT, 1280–1281
  - SATCOM, 1280
  - space and security budget, 1279
  - SSA, 1281
 Swedish Institute of Space Physics, 1281  
 Swedish National Space Agency, 1280  
 Swiss Data Cube (SDC), 1282  
 Switzerland
  - EO, ISR, 1282
  - PNT, 1283–1284
  - SATCOM, 1283
  - space and security budget, 1281
  - SSA, 1284
 Synthetic aperture radar (SAR), 582, 715, 1229, 1244, 1385  
 Syracuse III, 788, 1230, 1231  
 Syracuse IV, 789, 1231  
 Systeme Probatoire d'Observation du Ciel (SPOC), 1335
- T**
- TanDEM-X, 1239  
 Technology advantage, 1372  
 Technology Experiment Satellite (TES), 582  
 Techno-nationalism, 37  
 Tele commands
  - authentication, 255
  - availability, 255
  - confidentiality, 255
  - integrity, 255
  - sequencing, 255
 Telecommunication satellite, 874, 1351–1352  
 Tele-learning, 637  
 Telemak, 1231  
 Telemetry, 255–256  
 Telstar 1, 780



- Ten Propositions Regarding Spacepower*, 52
- TerraAM-1, 876
- TerraSAR-X satellite, 1109, 1238, 1239
- Thales Alenia Space Italy (TASI), 1244
- The Netherlands
- EO, ISR, 1272–1273
  - PNT, 1274–1275
  - SATCOM, 1273–1274
  - space and security budget, 1271
  - SSA, 1275
- Third-generation BeiDou system (BDS-3), 1390
- Threat intelligence, 932
- Threats in space systems
- change of strategic landscape, 867–869
  - early armed threats, 869–870
  - in orbit, 871–873
  - space deterrence, 879–880
  - space threats, 874–879
  - vulnerability of spacecraft, 874
- Thuraya Satellite Communication Company, 640
- Tiangong-1, 516
- Tianlian-1 04 satellite, 1387
- Tiantong-1 01 satellite, 1387
- Tianyuan-1, 1394
- Time of Closest Approach (TCA), 945
- TOPAZ satellites, 1155
- Top-level policy documents, 1370
- Tracking, telemetry, and control (TT&C), 534, 540
- Tracking and data relay satellite System (TDRSS), 1145
- Tracking and Imaging Radar (TIRA), 1242
- Trajectory Prediction, 979
- TRANSIT, 823
- Transparency-and confidence-building measures (TCBMs), 59, 61–64, 87, 89, 90, 347, 386, 395, 396, 504, 1544, 1548
- Treaty on European Union (TEU), 201, 1117
- Treaty on the Functioning of the European Union (TFEU), 200, 201
- Treaty on the Prevention of the Placement of Weapons in Outer Space, the Threat or Use of Force Against Outer Space Objects (PPWT), 88, 89, 586
- Trump, Donald, 368, 379, 381, 383
- Two line elements, 967
- U**
- UAE National Space Strategy 2030, 364
- UK Civil Space Strategy, 481
- UK Defence Equipment Plan, 1254
- UK National Space Policy, 480
- Ultra high frequency (UHF) follow-on (UFO) constellation, 1140
- UN Charter on Human Rights, 1073
- UN Committee on the Peaceful Uses of Outer Space (COPUOS), 597
- UN Covenant on Civil and Political Rights, 1073
- UN General Assembly (UNGA), 1094, 1100, 1101
- UNISPACE+50, 1550, 1554
- United Arab Emirates (UAE), 364
- space activities in, 23
- United Arab Emirates (UAE) approach, space and security, 623–625
- international space cooperation, 627–628
  - LTS guidelines, 642–650
  - national regulatory framework for, 625
  - SDGs, 634–642
  - Space2030 Agenda, 629–634
  - space economy, 628–629
- United Kingdom, 430–431
- EO, ISR, 1252–1253
  - military SATCOM, 788
  - PNT, 1255–1256
  - SATCOM, 1254–1255
  - space and security budget, 1252
  - space and security status, 479
  - SSA, 1256
  - strategic documents, space and security elements in, 479–481
- United Nations, 1538
- United Nations Charter, 81, 87
- United Nations Committee on the Peaceful Uses of Outer Space (UNCOPUOS), 7, 59, 63, 76, 79, 323, 520, 566, 627, 642, 644, 655, 672, 846–848, 1539, 1540
- international legal framework, 323–325
  - long-term sustainability of space activities on, 325–326
  - space debris mitigation guidelines, 1551
  - Working Group on the Long-Term Sustainability of Outer Space Activities, 326–331, 1551
- United Nations Convention on the Law of the Sea (UNCLOS), 78, 193, 1081
- United Nations Department of Economic and Social Affairs (UN DESA), 581
- United Nations Disarmament Commission (UNDC), 1539, 1540, 1547, 1548
- United Nations General Assembly (UNGA), 79, 1539
- UNGA First Committee, 1539, 1546

- UNGA Fourth Committee, 1540, 1546
  - United Nations Group of Governmental Experts (UN GGE), 1064
  - United Nations Institute for Disarmament Research (UNIDIR), 1539, 1540, 1543, 1546, 1555
  - United Nations Office for Disarmament Affairs (UNODA), 1539, 1546
  - United Nations Office for Outer Space Affairs (UNOOSA), 1066, 1539, 1540, 1546, 1554, 1561
  - United Nations Register of Conventional Arms (UNROCA), 191
  - United Nations Security Council, 83
  - United Nations Space Treaties, 79, 87, 90
  - United Rocket and Space Corporation, 394
  - United States, 361
    - commercialization of outer space, 350
    - military SATCOM in, 787
  - United States Munitions List (USML), 197, 198
  - United States Space Force (USSF), 54
  - United States Strategic Command (USSTRATCOM), 975
  - Unmanned aerial systems (UAS), 117
  - Unmanned aerial vehicles (UAV), 582, 948, 950, 967, 1253
  - Unmanned air traffic management (UTM), 947, 948, 950
  - Unmanned lunar mission, 502
  - UN Office of Outer Space Affairs, 1029
  - UN Peacekeeping, 557, 562
  - UN Remote Sensing Principles
    - free use and dissemination, 1097–1098
    - international law, 1100–1102
    - scope of application and security, 1095–1097
    - security limiting dissemination, 1098–1100
  - UN Security Council, 191, 668, 698
  - U.S. Air Force, 306
  - US–Australia Multidisciplinary University Research Initiative (AUSMURI), 1449
  - US export control regime, 194–195
    - dual-use goods, 195–197
    - military goods, 198–200
  - U.S. National Security Strategy, 114
  - US satellite hacking, 249
  - US space policy
    - Bush’s administration, 376, 378, 380
    - Carter’s administration, 375
    - Clinton’s administration, 377, 380
    - Dyna-Soar Program, 373
    - Eisenhower’s administration, 370, 372
    - Eisenhower’s fiscal policies, 372
    - Kennedy administration, 373
    - Massive Retaliation doctrine, 369
    - National Security Council (NSC)
      - Directive, 372
    - Nixon administration, 374
    - NSP, 368, 380, 382
    - NSS, 381
    - Obama’s administration, 378
    - Project RAND, 368
    - Project Vanguard, 371
    - Reagan’s administration, 375
    - SAINT interceptor program, 372, 374
    - SPD-1, 382
    - SPD-2, 382
    - SPD-3, 382
    - SPD-4, 383
    - STARFISH PRIME program, 374
    - Trump administration, 368
    - US military, 369
    - USSPACECOM, 377
  - US STRATCOMM, 596
  - Uzbekistan, economic and financial (E&F) operations, 176
- V**
- Van Allen belts, 1035, 1039
  - Vasiliev, Victor, 396
  - VEGA project, 1349
  - Very High Throughput Satellites (VHTS), 1070, 1072
  - Violent Extremist Organizations (VEOs), 378
  - Vision Plan of Iran, 604–606
  - Von Braun, Werner, 369, 371
  - Vulnerability, 748–750
- W**
- Wassenaar Arrangement on Export Controls, 190
  - Weaponization of outer space, 346
  - Weaponization of space, 869, 1332
  - Weapons of mass destruction (WMD), 396, 718
  - Western European Union
    - during 1955–2001, 403–405
    - during 1979–1999, 405–415
    - drafting a space policy, 414, 415
    - earth observation space policy, 411–414
    - earth observation system for defence, 409, 411
    - Military Committee, 406
    - Military Staff, 406, 414
    - ministerial level development, 407–408

- Western European Union (*cont.*)  
  Satellite Center, 407, 408, 411, 413, 415  
  Space Group, 406, 409–411, 414, 415  
  space group level development, 409  
White Paper on Defense and National  
  Security, 1335  
Wide-Area Augmentation System  
  (WAAS), 800  
Wideband global satcom, 1143–1144  
Wideband Global Satcom system (WGS), 1297  
Wideband Global System, 787  
Winged-rocket system, 288  
World Administrative Radio Conference  
  (WARC-63), 986  
World Meteorological Organization (WMO),  
  640, 663, 908, 1006  
World Radiocommunication Conference  
  (WRC-19), 986, 998, 999
- X**  
X-15 crash, 289  
Xenon ion propulsion system (XIPS), 1144  
X-ray flares, 1028, 1035  
Xtar-EUR, 790
- Y**  
Yaogan series satellites, 1385  
Yasniy Cosmodrome, 1185
- Z**  
Zephyr 8 HAPS program, 1253  
Zhuhai-1, 1386  
Ziyuan satellite series, 909, 1384  
Zombiesat, 878